

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE



# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

## ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

## VZÁJEMNÁ OVLIVŇOVÁNÍ WLAN SÍTÍ

INTERACTIONS BETWEEN WLAN NETWORKS

### BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

### AUTOR PRÁCE

AUTHOR

Eva Doleželová

### VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. Vladislav Škorpil, CSc.

BRNO 2020

# Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

**Studentka:** Eva Doleželová

**ID:** 177313

**Ročník:** 3

**Akademický rok:** 2019/20

**NÁZEV TÉMATU:**

## Vzájemná ovlivňování WLAN sítí

### POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou vzájemného ovlivňování WLAN sítí. Zaměřte se jak na rušení stejných typů WiFi, tak na rušení různých typů. Nejprve se věnujte problematice teoreticky, poté vytvořte zjednodušené hardwarové zapojení. S použitím vhodných programů simulujte vzájemné ovlivňování WLAN sítí. Výsledky simulací i fyzického modelu podrobte diskusi, porovnejte je a zhodnoťte. Vypracujte minimálně dvě laboratorní úlohy pro studenty včetně vzorových protokolů a manuálů pro učitele.

### DOPORUČENÁ LITERATURA:

[1] PUŽMANOVÁ, R. Moderní komunikační sítě A-Z. Computer Press, Brno 2007

[2] ŠKORPIL, V. Vysokorychlostní komunikační systémy. FEKT, Brno 2014

**Termín zadání:** 3.2.2020

**Termín odevzdání:** 8.6.2020

**Vedoucí práce:** doc. Ing. Vladislav Škorpil, CSc.

**Konzultant:** Ing. Pavel Mašek, Ph.D. (VUT Brno)

**prof. Ing. Jiří Mišurec, CSc.**  
předseda rady studijního programu

### UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## **Abstrakt**

Tato práce se zabývá vzájemným ovlivňováním WLAN sítí. Vysvětluje historii a následný vývoj bezdrátových technologií a poté se zaměřuje na současné WLAN sítě. Popisuje problematiku rušení ve WLAN sítích a parametry, které nedílnou součástí přispívají k vzájemnému rušení. Součástí práce je vypracování dvou laboratorních úloh. První úloha je realizována v programu Riverbed, ve kterém je sestavena topologie se třemi stejnými WLAN routery. Po otestování WLAN routerů je zobrazen graf popisující rušení v pásmu 2,4 GHz, kterého je dosaženo vhodným zvolením frekvenčního pásma, vysílacího výkonu a kanálu. Druhá laboratorní úloha je realizována v programu Iperf3, který je nainstalovaný na třech Raspberry Pi (RPi Zero, RPi 3 a RPi 4). Zahlcení sítě je docíleno pomocí skriptu wifijammer, který je nainstalován na RPi 4. V této druhé laboratorní úloze byly nejdříve ověřeny parametry přenosu a pomocí skriptu wifijammer byla odmítnuta služba. Pro testování druhé laboratorní úlohy byly zvoleny standardy IEEE 802.11b a IEEE 802.11n s ve frekvenčním pásmu 2,4 GHz. Testování probíhalo na routerech Mercusys, Netis, Tp-Link a Asus. Výsledky z testovacích scénářů byly přehledně zpracovány formou grafů.

## **Klíčová slova**

WLAN, Wi-Fi, Raspberry Pi, Wifijammer, Iperf3

## **Abstract**

This bachelor thesis deals with the possible interferences caused by the parallel running WLAN networks. It explains the history and subsequent development of wireless technologies and then focuses on current WLAN networks. It describes the problem of interference in WLAN networks and parameters that contribute to mutual interference. Practical part of this thesis consists of two laboratory exercises. The first task is implemented in the Riverbed program, in which a topology with three identical WLAN routers is assembled. After testing the WLAN routers, a graph describing the interference in the 2.4 GHz band is displayed, which is achieved by a suitable choice of frequency band, transmission power and channel. The second laboratory task is implemented utilizing the Iperf3 program, which is installed on three Raspberry Pi's (RPi Zero, RPi 3, and RPi 4). Network congestion is achieved using the wifijammer script, which is installed on RPi 4. In this second laboratory task, the transmission parameters were first verified and the service was denied using the wifijammer script. For evaluation of the second laboratory task, the IEEE 802.11b and IEEE 802.11n utilizing the frequency band 2,4 GHz were chosen. For testing, the following routers were used: Mercusys, Netis, Tp-Link and Asus routers. Once the measurements were over, all the data was processed and included as charts.

## **Keywords**

WLAN, Wi-Fi, Raspberry Pi, Wifijammer, Iperf3

Doleželová, Eva. *Vzájemná ovlivňování WLAN sítí*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2020. 127 s. Vedoucí bakalářské práce doc. Ing. Vladislav Škorpil, CSc.

## Prohlášení

„Prohlašuji, že svou bakalářskou práci na téma Vzájemná ovlivňování WLAN sítí jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne:.....

.....

podpis autora

## **Poděkování**

Děkuji vedoucímu bakalářské práce doc. Ing. Vladislavu Škorpilovi, CSc., za velmi užitečnou metodickou pomoc a cenné rady při zpracování práce. Také bych chtěla poděkovat panu Ing. Pavlovi Maškovi, Ph.D. za konzultace a pomoc při zpracování bakalářské práce. Ještě bych chtěla poděkovat své rodině za podporu v průběhu celého studia.

V Brně dne .....

.....

podpis autora

Tato práce vznikla jako součást klíčové aktivity KA6 - Individuální výuka a zapojení studentů bakalářských a magisterských studijních programů do výzkumu v rámci projektu OP VVV Vytvoření double-degree doktorského studijního programu Elektronika a informační technologie a vytvoření doktorského studijního programu Informační bezpečnost, reg. č. CZ.02.2.69/0.0/0.0/16\_018/0002575.



EVROPSKÁ UNIE  
Evropské strukturální a investiční fondy  
Operační program Výzkum, vývoj a vzdělávání



Projekt je spolufinancován Evropskou unií.



# Obsah

Úvod.....	6
1 Síť .....	7
1.1 Úvod do sítí.....	7
1.3 Vznik bezdrátové komunikace.....	9
1.4 Bezdrátové technologie .....	9
1.4.1 Bezlicenční pásmo .....	9
1.4.1.1 ZigBee .....	9
1.4.1.2 Bluetooth .....	11
1.4.1.3 WiFi .....	13
1.4.1.4 Ultra-wideband (UWB od WiMedia Alliance) .....	13
1.4.2 Licenční pásmo .....	15
1.4.2.1 WiMAX (Worldwide Interoperability for Microwave Access) .....	15
1.4.2.2 První generace (1G).....	16
1.4.2.3 Druhá generace (2G) .....	16
1.4.2.4 Přechodová generace (2,5G) .....	17
1.4.2.5 Třetí generace (3G).....	17
1.4.2.6 Čtvrtá generace (4G) .....	19
1.4.2.7 Pátá generace (5G) .....	19
1.4.2.8 Srovnání vlastností bezdrátových technologií.....	21
1.4.2.9 Porovnání mobilních sítí.....	22
1.5 Historie WLAN.....	23
1.6 Bezdrátová technologie WLAN.....	24
2 Současné požadavky na WLAN .....	25
2.2 Parametry WLAN sítí .....	25
2.2.1 Přenosová rychlost.....	25
2.2.2 Antény.....	25

2.2.3 QoS, kvalita služby ve WLAN .....	26
2.2.4 Výkon.....	28
2.2.5 Pořizovací cena .....	28
2.3 Standardy WLAN sítí .....	30
2.3.1 IEEE 802.11 (legacy) – 1-2 Mbps .....	30
2.3.2 802.11a – 1,5-54 Mbps .....	30
2.3.3 802.11b – 11 Mbps .....	31
2.3.4 802.11g – 54 Mbps .....	31
2.3.5 802.11n – 300 Mbps .....	31
2.3.6 802.11ac – 6,933 Gbps .....	32
2.3.7 802.11ad – 6,756 Gbps .....	32
2.3.8 802.11af a 802.11ah.....	33
2.4 Tabulka srovnání jednotlivých standardů .....	33
2.5 Zabezpečení WLAN .....	33
2.5.1 SSID (Service Set Identifier) .....	34
2.5.2 ESSID (Extended Service Set Identification) .....	34
2.5.3 Šifrování WEP (Wired Equivalent Privacy) .....	34
2.5.4 Šifrování WPA (Wi-Fi Protected Access) .....	34
2.5.5 Šifrování WPA2.....	35
2.5.6 Šifrování WPA3.....	35
2.6 Použití WLAN ve firmách .....	37
2.7 Použití WLAN v domácnostech .....	37
3 Teoretický návrh měření .....	38
3.1 Rušení WLAN sítí .....	38
3.2 Použité programy pro realizaci laboratorních úloh.....	38
3.2.1 Riverbed.....	38
3.2.2 Iperf3.....	38
3.2.3 Scapy.....	39

3.3 Předpokládaný závěr .....	40
4 Laboratorní úlohy .....	42
4.1 Vypracování laboratorních úloh .....	42
4.2 Semestrální laboratorní úloha – 1. Laboratorní úloha .....	43
4.3 Druhá laboratorní úloha – HW sestavení.....	53
5 Závěr .....	68

## Seznam obrázků

Obr. 1: Základní struktura sítě [1] .....	7
Obr. 2: Vývoj mobilních technologií [24] .....	20
Obr. 3: Sestavení úlohy.....	44
Obr. 4: Celková propustnost jednotlivých routerů.....	47
Obr. 5: Propustnost routeru 1 .....	48
Obr. 6: Propustnost routeru 2.....	48
Obr. 7: Propustnost routeru 3.....	49
Obr. 8: Zpoždění .....	49
Obr. 9: Zapojení laboratorní úlohy .....	53
Obr. 10: Příkaz na RPi 3 (iperf3Server).....	55
Obr. 11: Příkaz na ověření propustnosti .....	55
Obr. 12: Příkaz na ověření zpoždění.....	55
Obr. 13: Postup při zpracování dat v aplikaci Bitvise .....	57
Obr. 14: Přenos TCP pro router Mercusys s použitým standardem 802.11 n. ....	58
Obr. 15: Přenos TCP pro router TP-Link s použitým standardem 802.11 n. ....	58
Obr. 16: Přenos UDP pro router Mercusys s použitým standardem 802.11 n.....	59
Obr. 17: Přenos UDP pro router TP-Link s použitým standardem 802.11 n.....	59
Obr. 18: Přenos TCP pro router Mercusys s použitým standardem 802.11 n.....	60
Obr. 19: Přenos TCP pro router Netis s použitým standardem 802.11 n.....	61
Obr. 20: Přenos UDP pro router Mercusys s použitým standardem 802.11 n.....	61
Obr. 21: Přenos UDP pro router Netis s použitým standardem 802.11 n.....	62
Obr. 22: Zobrazení MAC adresy zařízení RPi.....	63
Obr. 23: Příkaz pro zahlcení standardu 802.11 b.....	64
Obr. 24: Přenos TCP pro router Mercusys s použitým standardem 802.11 n. ....	65
Obr. 25: Přenos UDP pro router Mercusys s použitým standardem 802.11 n.....	65
Obr. 26: Přenos UDP pro router Asus s použitým standardem 802.11 n. ....	66
Obr. 27: Přenos TCP pro router Asus s použitým standardem 802.11 n.....	66

## Seznam tabulek

Tab. 1: Vývoj technologie Bluetooth [55] .....	12
Tab. 2: Porovnání bezdrátových technologií část 1 .....	21
Tab. 3: Porovnání bezdrátových technologií část 2 .....	21
Tab. 4: Porovnání mobilních sítí.....	22
Tab. 5: Srovnání standardů 802.11 [30] .....	33

# ÚVOD

Technologie WiFi (Wireless Fidelity) je standard, který využívá bezdrátové připojení v počítačových sítích. WiFi sítě jsou dnes používány ke dvěma účelům a to jako korporátní sítě a jako veřejné přístupové sítě k Internetu. Čím dál více roste poptávka po rychlejší připojení, proto jsou nároky na výkon WLAN (Wireless LAN) větší.

WiFi sítě podporují několik standardů IEEE 802.11, které publikoval mezinárodní standardizační institut. Tyto standardy se liší frekvenčním pásmem, maximální rychlostí, alokovanou šířkou pásma, modulací či vysílacím výkonem. V dnešní době, v téměř každé domácnosti, je připojení k Internetu realizováno pomocí WLAN. Běžný uživatel si není vědom možných kolizí s ostatními WLAN v jeho okolí. Proto je v dnešní době snaha seznámit studenty s případnými kolizemi WLAN sítí a jejich možným řešením.

Tato bakalářská práce se zabývá problematikou vzájemného ovlivňování WLAN sítí s bližším zaměřením na zpoždění a propustnosti standardů WiFi. První kapitola obsahuje stručný úvod do sítí, bezdrátových technologií a historii vzniku sítí. Druhá kapitola se věnuje současným WLAN sítím, blíže popisuje parametry WLAN sítí, standardy WLAN sítí, jejich zabezpečení a použití v domácnostech a firmách. Obsahem třetí kapitoly je teoretický návrh měření, popis rušení a programů testujících vzájemné ovlivnění WLAN sítí. Na tento návrh měření přímo navazuje čtvrtá kapitola, která je věnována realizaci laboratorních úloh. Čtvrtá kapitola se věnuje vypracování laboratorních úloh, sestavení softwarové topologie v programu Riverbed, reálné komunikační topologie topologie s využitím Raspberry Pi 3, Raspberry Pi Zero a Raspberry Pi 4 a předpokládaného závěru. Pátá kapitola se věnuje závěru z měření laboratorních úloh a jejím srovnáním s předpokládaným závěrem z části 4. Laboratorní úlohy se věnují ovlivněním WLAN sítí ve frekvenčním pásmu 2,4 GHz. Zabývají se ovlivněním signálu třech WiFi routerů s různým frekvenčním pásmem, použitým standardem a maximální přenosovou rychlostí.

# 1 SÍŤ

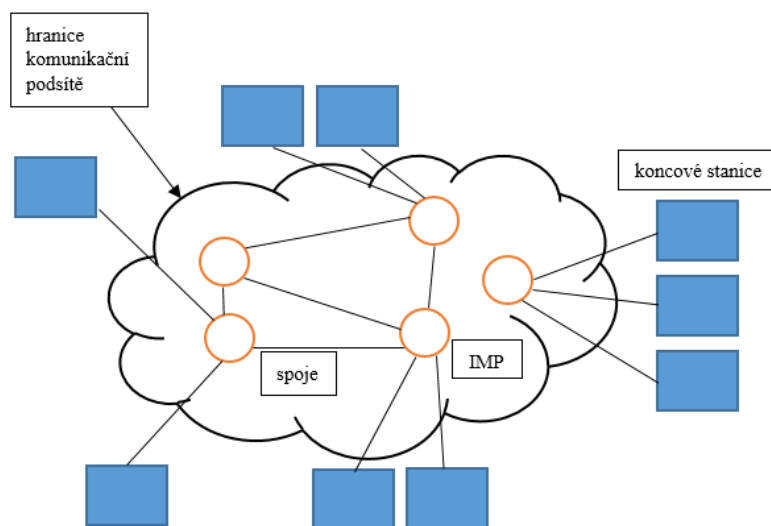
V současnosti je telekomunikace prezentována pouze digitálními technologiemi. Analogové sítě jsou dnes využívány pouze okrajově. Důvodem upřednostnění digitálních technologií je jejich všestranné zpracování informací a flexibilnější komunikační systémy, které umí reagovat na výpadky dílčích síťových prvků. [28]

## 1.1 Úvod do sítí

Spoje a přepojovací prvky jsou dvě základní komponenty sloužící k propojení koncových stanic. Pokud je realizován přenos zpráv mezi dvěma místy bez kladení důrazu na použité prostředky a druh přenosů, pak se jedná o spoje.

Přepojovací prvky umožňují propojení dvou a více spojů. Pro datové přenosy je využit přepojovací prvek IMP (Interface Message Processor). Přes IMP probíhá veškerý přenos mezi počítači. [1]

Základní struktura sítě je vyobrazena na Obr.1 [1]



Obr. 1: Základní struktura sítě [1]

Sítě se dále dělí podle topologie na dvoubodové spoje, do kterých patří:

- a) topologie typu hvězdy,
- b) topologie typu kruhu,

- c) topologie typu stromu,
- d) topologie typu úplného polygonu,
- e) topologie typu propojených kruhů,
- f) obecná topologie.

Dále se dělí na kanály s všesměrovým vysíláním (broadcast) dělící se dále na sběrnici a rádiové spojení.

Podle velikosti se síť dělí:

- a) Personal Area Network (PAN),
- b) Local Area Network (LAN),
- c) Metropolitan Area Network (MAN),
- d) Wide Area Network (WAN).

Personal Area Network (PAN) jsou sítě využívané jednou osobou nebo nízkým počtem osob. Využívané jsou zde nižší přenosové rychlosti v jednotkách (Mbit/s). V případě Local Area Network (LAN) je komunikace zprostředkována v rámci jedné budovy nebo blízkých budov. Využívá se několik přenosových rychlostí v jednotkách (Mbit/s), ale i rychlosti v jednotkách (Gbit/s). Metropolitan Area Network (MAN) propojuje lokální sítě v městské zástavbě. Přenosová rychlost je v (Gbit/s). Wide Area Network (WAN) má největší působnost. Spojuje LAN a MAN sítě po celém kontinentu.

Sítě se dále mohou dělit podle přepojování:

- a) komutační síť,
- b) paketovou síť.

Další možné rozdělení je podle postavení uzlů:

- a) Peer-to-peer (P2P),
- b) Klient-server.

Podle druhu přenášených signálů je možné síť dělit na analogovou a digitální. [7]



## **1.3 Vznik bezdrátové komunikace**

Mnoho vědců se odjakživa podílelo na rozvoji komunikačních technik. Kabelová telegrafie byla prvním elektrickým komunikačním systémem. Tu zdokonalil americký malíř Samuel Morse a patentoval ji v roce 1938. Samuel Morse v roce 1942, s použitím oddělených talířů ponořených ve vodě na dvou březích demonstroval bezdrátovou komunikaci. V tomto případě se jednalo o bezdrátovou komunikaci vedením. Pomocí indukční techniky v letech 1866 až 1873 přenášel telegrafické zprávy na vzdálenost 18 mil Mahlon Loomis. K rozvoji bezdrátové komunikace však nejvíce přispěl Guglielmo Marconi. Zasláním Morseovy zprávy z Anglie, přes Atlantik až do Kanady v roce 1901 začala nová éra bezdrátové komunikace. Bezdrátová komunikace, která dnes spojuje celý svět má počátek v práci Marconiho, Morse a mnoho dalších před více než sto lety. [6]

## **1.4 Bezdrátové technologie**

Tato kapitola rozděluje bezdrátové technologie na bezlicenční a licenční pásmo.

### **1.4.1 Bezlicenční pásmo**

Bezlicenční pásmo je pro bezdrátové technologie pásmo o velikosti 2,4 GHz. Jedná se o pásmo nelicencované. Pro toto pásmo je typické, že pro jeho využívání není potřeba povolení. Nevýhodou je velké vytížení a vzájemné rušení připojených zařízení.

#### **1.4.1.1 ZigBee**

ZigBee je jednou z bezdrátových technologií, která je využívána v osobních sítích PAN (Personal Area Network). Má označení IEEE 802.15.4. Tento otevřený standard se vyvíjel už od roku 1999 a měl několik cílů. Měl být spolehlivý, bezpečný, levnější než ostatní bezdrátové technologie a s nízkou spotřebou. Tato technologie měla být využita ke komunikaci mezi zařízeními a k monitoringu a kontrole různých zařízení. K vývoji a správě technologie ZigBee vznikla firma ZigBee Alliance, která byla založena v roce 2002. Výhody technologie ZigBee jsou nízká cena na pořízení, spolehlivost, nízká spotřeba energie, možnost vyššího zabezpečení a v neposlední řadě je to otevřený celosvětový standard. [21]

1 Další technologie pracující na stejném principu pro bezdrátový přenos je bezdrátové USB (Wireless USB), které spojuje dvě zařízení pomocí USB. Touto technologií je možné propojit zařízení jako externí disk, myš, fotoaparát a mnoho dalších. Dosahuje přenosových rychlostí 54 Mbit/s. [1]

---

1 Wireless USB – Standard pro obsluhu bezdrátových periferií. Založen na stejné technologii pro bezdrátový přenos jako technologie Zigbee.[12]

#### 1.4.1.2 Bluetooth

Jedna z možností jak připojit bezdrátová zařízení k síti PAN (respektive WPAN) je za pomoci Bluetooth. Je to jeden ze standardů IEEE 802.15.1, který pracuje na krátkou vzdálenost podobně jako ZigBee, za použití rádiových vln. Bluetooth využívá frekvenčního pásma v rozsahu 2,4 až 2,4835 GHz s použitím až 79 rádiových kanálů a má modulaci FHSS (Frequency Hopping Spread Spectrum). [22] [23] Přístroje, které využívají Bluetooth můžeme rozdělit do čtyř výkonostních tříd. První třída má maximální povolený výkon 100 mW což odpovídá 20 dBm za využití dosahu až 100 metrů, zatímco čtvrtá třída má povolený výkon 0,5 mW, což odpovídá -3 dBm, a dosah okolo půl metru. [22] Mezi hlavní výhody technologie Bluetooth se může zařadit jeho nízká pořizovací cena, malý vysílací výkon, snadná obsluha a jeho jednoduchá implementace. Vznik této technologie se datuje roku 1994. V tomto roce švédská firma Ericsson, která vyráběla mobilní telephony, hledala řešení, kdy se nahradí sériové rozhraní RS-232. [22] Za tímto účelem vznikla o čtyři roky později skupina Bluetooth special. Cílem této skupiny bylo vytvoření takové bezdrátové technologie, které nebude vadit nekompatibilita různých zařízení, která využije technologii na krátkou vzdálenost, a která bude mít co nejmenší energetické nároky. V roce 1999 se objevila první verze takzvaná Bluetooth verze 1.0 a 1.0a, která se díky mobilním zařízením jako jsou mobilní telefony, tiskárny pro bezdrátový přenos, klávesnice a myši, začala velice rychle šířit. Netrvalo dlouho a byla vydána verze 1.0b, která měla za úkol opravit chyby, které se objevili v její předešlé verzi. Verze 1.1 vydaná v roce 2001 měla přidáný indikátor síly signálu RSSI. Verze 1.2 přinesla zvýšení rychlosti a to na hodnotu až 721 kb/s, zlepšení kvality hlasu a modulaci AFH, která zlepšovala odolnost proti rádiovému rušení. Bluetooth verze 2.0+EDR zlepšovala propustnost pomocí metody EDR. Přenosová rychlost se mohla zvýšit a to až na hodnotu 2,1 Mb/s.

Roku 2007 vyšla verze 2.1+EDR, která se zaměřila hlavně na bezpečnost a zlepšila spárovatelnost zařízení. Jednou z největších změn byla verze z roku 2009. Bluetooth verze 3.0 +HS s přenosovou rychlostí až 24 Mbit/s. Toto připojení se, ale realizovalo pomocí souběžného připojení standardu 802.11. Poté přišla verze 4.0, kde bylo cílem dosažení minimální energetické zátěže pro přenos. Roku 2013 byla vydána verze Bluetooth 4.1, která zvyšovala odolnost proti technologii LTE. O rok později verze Bluetooth 4.2 přinesla možnosti zabezpečeného připojení a zvětšenou délku paketu. Jedna

z posledních verzí vydaná roku 2016 verze Bluetooth 5, která souvisí s internetem věcí (IoT). Poslední technologie Bluetooth je vydaná v roce 2019 a je využívána pro zjišťování polohy zařízení. [22]

Vývoj technologie Bluetooth od roku 2002 do roku 2019

Tab. 1: Vývoj technologie Bluetooth [55]

Term	Specification	Meaning (Key features)
BR	1.1 (2002)	Basic Rate (1 Mbit/s)
EDR	2.0 (2004)	Enhanced Data Rate (2 and 3 Mbit/s)
HS	3.0 (2009)	High Speed (alternate MAC/PHY)
LE	4.0 (2010)	Low Energy (1 Mbit/s ultra low power)
Bluetooth Smart	4.0	Single-mode, LE-only radio
Bluetooth Smart Ready	4.0	Dual-mode, BR/EDR and LE dual radio
Bluetooth 4.1	4.1 (2013)	Incremental software update to bluetooth v4.0, and not a hardware update
Bluetooth 4.2	4.2 (2014)	Older Bluetooth hardware may receive 4.2 features such as Data Packet Length Extension and improved privacy via firmware updates
Bluetooth 5	5.0 (2016)	New features are mainly focused on emerging Internet of Things technology
Bluetooth 5.1	5.1 (2019)	Angle of Arrival (AoA) and Angle of Departure (AoD) which are used for location and tracking of devices

### **1.4.1.3 WiFi**

WLAN se začaly používat, aby pokryly dané území signálem. Jejich standard je IEEE 802.11, ale obecně jsou známé pod zkratkou Wi-Fi (Wireless Fidelity). Tato technologie je dnes součástí snad každé domácnosti, restaurace, firmy a obchodů kde se na ni mohou připojit uživatelé pomocí notebooků nebo mobilních telefonů a různých dalších bezdrátových zařízení. Jako první je uvedena verze standardu IEEE 802.11 označována jako legacy, která v roce 1997 představovala náhradu za pevnou síť ethernet. Netrvalo dlouho a začaly se vyvíjet i další verze, které se odlišovaly malým latinským písmenem jako IEEE 802.11a, b, g, n, ac, ad, af, ah, ax a ay. Tyto systémy pracují v ISM, což je bezlicenční frekvenční pásmo, které je většinou 2,4 GHz. I když je pásmo bezlicenční tak podléhá určitým omezením, jako je například jeho maximální vyzářený výkon, který nesmí překročit hodnotu 100 mW a jeho výkonová spektrální hustota, která může být maximálně 10 dBm/1 MHz. Pásmo 2,4 GHz v současné době využívají i další bezdrátové komunikační technologie jako ZigBee, Bluetooth, mikrovlnné trouby ale i některé lékařské přístroje. Proto je v tomto pásmu pro Evropu přiděleno 13 rádiových kanálů, pro Ameriku a Kanadu 11 rádiových kanálů. V 5 GHz pásmu je přiděleno pro Evropu 19 rádiových kanálů, pro Ameriku a Kanadu 24 rádiových kanálů. [48] Z těchto 13 kanálů se navzájem nepřekrývají pouze 3. Jedná se o kanály 1, 6 a 11. Použití bezlicenčního pásma znamenal velký posun dopředu, ale nesl sebou i jednu podstatnou nevýhodu. U pásma 2,4 GHz docházelo k přepřínování, a proto se začalo využívat i frekvenční pásmo 5 GHz, které je pro uživatele bezlicenční. Obecně to však znamená nutnost frekvenčního plánování a refarmingu spectra nejen pro pásmo ISM 2,4 GHz. [8]

### **1.4.1.4 Ultra-wideband (UWB od WiMedia Alliance)**

Ultra-wideband (UWB) je bezdrátová technologie, využívající Čas letu, který je vhodný pro přesnější měření vzdálenosti. Technologie UWB disponuje několika vlastnostmi, mezi které lze zařadit odolnost proti hluku, odolnost vůči šíření signálu větším množstvím cest, lokalizační přesnost, možnost využití nízké výkonových vysílačů a ostatní komunikační systémy jej nemohou rušit. Technologie UWB využívá standard IEEE 802.15.4a, šířku pásma 500 MHz, provozní frekvenci 3-7 GHz a celkem 16 rozhlasových kanálů pracujících v nízkém a vysokém kmitočtovém pásmu. Celkem tento standard podporuje tři kmitočtová pásma. Revize standardu IEEE 802.15.4 -2011, která vyšla v

roce 2011, nejen blíže určila nízké, vysoké a sub-gigahertzové kmitočtové pásmo, ale také datové rychlosti, které technologie UWB využívá. Tyto datové rychlosti na fyzické vrstvě (PHY) jsou 110 kbps, 850kbps, 6,8 Mbps a 27 Mbps. U UWB se využívá soustava impulzů k přenosům informací než jak je tomu u jiných systémů, kde se využívá modulovaná sinusová vlna. Díky této vlastnosti je vhodný pro aplikace, které pracují s přesným určováním rozsahu. Příjímač může velmi přesně určit čas příchodu signálu a to díky strmé náběžné hraně pulzu. Tyto pulzy jsou velice úzké běžně okolo dvou nanosekund. UWB pulzy se také dají rozlišit v hlučných prostorech kde je signál odolný vůči vícecestným efektům. To jsou jedny z výhod UWB s porovnáním s tradičními úzkopásmovými signály co se týče dosahu. Pro své vlastnosti jako je přesnost a nízká spotřeba energie se využívá UWB na místech jako jsou nemocnice. [13]

## 1.4.2 Licenční pásmo

Licenční pásmo využívá pásma od 4 GHz až do 42 GHz. Využívání tohoto pásma je podmíněno licencí, kterou si musí uživatel zaplatit. Značnou výhodou licencovaných pásem je ochrana proti rušení a velkokapacitní přenos.

### 1.4.2.1 WiMAX (Worldwide Interoperability for Microwave Access)

WiMAX byl využíván pro širokopásmé připojení k Internetu pro bezdrátové WAN sítě a tedy pro vzdálenosti desítek kilometrů. [31] Tato technologie je ve standardu IEEE 802.16 podrobně vylíčena. Ke svému šíření používá mikrovlny, používá licencovaná pásma, která jsou pod 11 GHz. Pro Evropu používán licencovaný 3,5 GHz a nelicencovaný 5,8 GHz kmitočet. Ve srovnání s Wi-Fi je u technologie WiMAXu menší rušení a to díky použití licencovaných pásem. Má také lepší podporu QoS. WiMAX, Wi-Fi a Bluetooth mají jedno společné a to je společnost IEEE, která tyto technologie vyvíjí. Tyto technologie nejsou navzájem konkurence, ale každá je určená do daného prostředí, ve kterém pracuje. Konkrétně WiMAX je použit na místě, kde uživatel potřebuje mít velkou oblast pokrytí než je třeba u Wi-Fi a také na místě, kde bude mít dedikovanou přenosovou rychlost. Toto řešení je pro poskytovatele internetu, kteří musí zaručit připojení i v odlehlých oblastech. Využít ho mohou i firmy a velké instituce jako třeba školy. Rok 2004 přinesl standard 802.16d, kde byly použity certifikované produkty a kde byl výběr z jeho fyzických vrstev, které obsahovaly například OFDM (Orthogonal Frequency Division Multiplexing) nebo single carrier. Hodnota frekvence se snížila pod 11 GHz. Kromě těchto možností zde byla i myšlenka využití nových anténích technik jako space time coding nebo spatial multiplexing. V roce 2005 se objevila verze 802.16e, kterou bylo možné využít s použitím mobilního zařízení. Zavedla se zde nová technologie Scalable-OFDMA, která na fyzické vrstvě upravila vlastnosti šířek kanálů pomocí standardizace. Nevýhodou zde bylo, že maximální rychlost, propustnost a cena se nevyrovnala verzi 802.16d. V roce 2011 se objevila verze 802.16m, která se nazývá WiMAX 2. U této verze došlo ke zlepšení všech parametrů z předchozí verze a to díky tomu, že splnila požadavky IMT-Advanced. S tím je spojeno navýšení maximální rychlosti přenosu až na 1 Gbit/s pro mobilní zařízení. [31]

#### **1.4.2.2 První generace (1G)**

1G (První generace), která vznikla v 80. letech 20. století, byla určena pro provoz mobilních služeb. V této době byl vynalezen i první mobilní telefon. Tato technologie byla analogová a hlavním úkolem byl přenos hlasu. Analogové systémy a služby první generace (1G):

NMT (Nordic Mobile Telephone) začal fungovat v roce 1979 a to na území Švédska a Norska, šlo o první komerčně využívaný analogový mobilní systém.

AMPS (Analog Mobile Phone System) provoz byl zahájen na území USA v roce 1982.

TACS (Total Access Communication System) byl určen pro Velkou Británii, ale nakonec se začal používat v Asii a byl určen i pro Pacifik. [3]

#### **1.4.2.3 Druhá generace (2G)**

2G (Druhá generace), která započala svoji éru v 90. letech 20. století, na rozdíl od první generace už uměla využít digitálního přenosu. Byla založená na přepínání okruhů (dnešní technologie jsou založené na přepínání paketů), pořád se zaměřovala na hlasové služby a to je i důvod proč její propustnost je do 20 kbit/s. Mezi nové technologie se řadí:

GSM (Global System for Mobile Communications), je to jedna z mobilních technologií, která využívá TDMA (Time Division Multiple Access) a FDMA (Frequency Division Multiple Access), což je časový a kmitočtový multiplex. Využívá principu přepojování okruhů. Systém GSM je převážně využíván pro hlasový přenos.

CDPD (Cellular Digital Packet Data), využívána k rozšíření pevných datových sítí s přenosovou kapacitou až 19,2 kbit/s. Používala hlasový analogový kanál o šířce pásma 30 kHz. Jeden kanál využívá naráz více uživatelů.

TDMA (Time Division Multiple Access), využívá jednu frekvenci, na které je více uživatelů. Tato metoda využívá přepojování okruhů.

CDMA (Code Division Multiple Access), u této technologie je to podobné jako u TDMA, je zde rozdíl v tom, že CDMA využívá více frekvencí a ne jenom jednu jako je to u TDMA a CDMA využívá přepojování paketů a ne okruhů jak je tomu u technologie TDMA a u technologie GSM. [3]



#### **1.4.2.4 Přejchodová generace (2,5G)**

2,5G (Generace přechodová) byla uvedena v roce 2001. Přejchodová generace byla takovým mezistupněm mezi 2 generací, která byla založená na přepínání okruhů, a generací třetí (3G), která je založena na přenosu dat a hlasu. [49] Tato technologie podporuje nejenom hlasovou komunikaci, ale podporuje i přenos dat a tedy textovou komunikaci a nově i přístup k internetu, který má rychlost až 115 kbit/s. K nejdůležitějším technologiím přechodové generace se řadí GPRS (General Packet Radio Service) a EDGE (Enhanced Data Rates for GSM Evolution).

GPRS (General Packet Radio Service) – slouží jako nadstavba GSM a využívá paketového přepínání. Tato technologie je určena pro připojení k internetu na delší časový interval. Bohužel to nedokáže širokopásmově, ale pouze v určitém frekvenčním spektru. Teoretická rychlost mohla být až 115 až 160 kbit/s i když ve skutečnosti to spíše bylo něco okolo 20 až 40 kbit/s. Pokles je dán reálným prostředím, ve kterém je nutné brát v potaz zahlcení, překážky, rušení ostatními stanicemi v okolí. GPRS využívá mnohem efektivněji síť než technologie GSM.

EDGE (Enhanced Data Rates for GSM Evolution) – je to vylepšení sítě GSM/GPRS. Tato technologie má už blíže ke třetí generaci například tím, že využívá modulaci s trojnásobnou datovou rychlostí při ideálních podmínkách. Jedná se o modulaci PSK – Phase Shift Keying. Jsou zde omezení, která jsou stejná jak u GPRS. [3]

#### **1.4.2.5 Třetí generace (3G)**

3G (Třetí generace) mobilních sítí, která se využívá i dnes. Pro nemobilní zařízení (koncové) zajistí rychlost až 2 Mbit/s. Při běžné chůzi může dosáhnout rychlosti až 384 kbit/s. Při jízdě autem se tato rychlost pohybuje okolo 144 kbit/s. Tato síť jako první využívá širokopásmové služby. 3G obsahuje celou řadu různých rádiových technologií, které jsou využívány pro provoz této mobilní sítě. Jedna z technologií, která patří do rodiny 3G je technologie UMTS. [3]

UMTS – Všechny jeho prvky jsou změněné za účelem vylepšení kvality služeb (QoS). Změněný je například řadič rádiové sítě RCN (Radio Network Controller), u GSM se využíval řadič základnové stanice BSC (Binary Synchronous Communication), který používala 2G a 2,5G. Slouží nejen pro hlasové služby, ale i pro datový přenos, dokáže rozlišit požadavky provozu a to díky QoS. Pro zvýšení rychlosti přenosu dat byl uveden

doplněk HSDPA (High-Speed Downlink Packet Access). Díky doplňku HSDPA bylo možné přenášet data rychlostí 1,8-14,0 Mb/s. Avšak s nástupem sociálních sítí, kde je hlavní myšlenka sdílení fotek a videí, přišli vývojáři s novou metodou, která zrychlí nahrávání dat na 5,76 Mb/s.

Tato technologie se nazývá HSUPA (High-Speed Uplink Packet Access). Spojením těchto dvou technologií vznikla technologie HSPA. [49] [3]

HSPA – je kombinací HSDPA a HSUPA. Nenavysahuje jenom zpětný směr komunikace a to od uživatele zpět k síti, ale i rychlost, která je od 1 až do 5 Mbit/s a zpoždění od 5 do maximálně 30 ms. HSPA ke svému provozu využívá u vysílače i přijímače více antén (technologie MIMO - Multiple Input, Multiple-Output). Tyto antény jsou v prostoru směřovány ortogonálně a to znamená, že rychlost daného přenosu lineárně poroste s počtem antén, které budou u vysílače. [3]

#### **1.4.2.6 Čtvrtá generace (4G)**

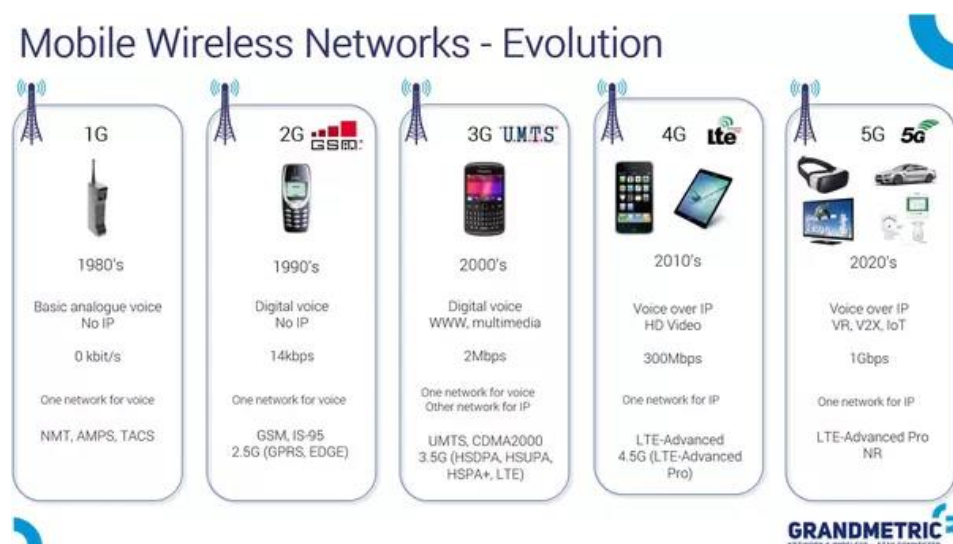
4G (Čtvrtá generace) umožnila vylepšení kvality hovoru a datových přenosů. [50] Vyvíjecí standard LTE, který byl použit ve 4G, měl však přenosovou rychlost nižší a nebylo možné jej použít na všech mobilních zařízeních. Kvůli problému s nižší přenosovou rychlostí byl uveden standard LTE-Advanced, který tento problém vyřešil. Zásadním rozdílem mezi technologiemi LTE a LTE-Advanced je tedy v přenosové rychlosti [51]. Ve čtvrté generaci je zásadní rozdíl v komunikaci All-IP a v požadavku na co nejméně prvků v síti. [29] LTE je složeno z EPC (Evolved Packet Core) a UTRAN (Terrestrial Radio Access Network). V LTE a LTE-Advanced jsou základnové stanice zvané eNodeB (eNB). ENodeBs jsou propojeny v rámci transportní sítě pomocí rozhraní X2. V síti LTE se provádí směrování datových i hlasových služeb. Tyto data se nerozlišují a putují stejnou sítí. V tomto ohledu je tohle jedna z hlavních výhod sítě LTE. Jako další součást sítě jsou zde uvedeny MME (Mobility Management Entity) prvky, které slouží pro autentizaci jednotlivých uživatelů a dohled nad stavy relací. S-gateway má za úkol směrovat přenášená data přes přístupovou síť. PDN gateway se stará o vnější komunikaci ale i o kvalitu služeb a o kontrolu paketů. Tato nová generace využívá OFDM širokopásmovou modulaci, která pro daný přenos používá nejenom nosnou frekvenci, ale i subnosné frekvence ve svém spektru. Další modulace je umožněna díky QPSK a 16/64-QAM. Aby se mohla přenosová rychlost zvýšit na několikanásobek původní, byla využita technologie MIMO, u které terminály využily více antén a komunikovaly se základnovými stanicemi. Jednotlivé antény mohou být použity pro datové streamy. Aby uživatel mohl přecházet ze sítě 4G do sítě 3G, muselo docházet k odpojení sítě a dlouhému připojování a ověřování k síti druhé. Přechod z 4G do 3G bez výpadku a ztráty IP adresy nebyl možný. Tento uživatel se se svým mobilním zařízením dostal na místo, kde není signál LTE, ale přesto by se mohl připojit na síť nižší generace. [29]

#### **1.4.2.7 Pátá generace (5G)**

5G (Pátá generace), pro kterou byl v roce 2017 vydán standard R15, má za cíl připojit nejlépe všechny mobilní zařízení k síti. K tomu jí má pomoci připojení, které má mít přenosovou rychlost (hypoteticky) až 20 Gb/s a pro městské využití i rychlost blízká hranici 100 Gbit/s. [11]

Maximální zpoždění u těchto sítí je 10 ms. [11] To je docíleno díky technologii MEC (Mobile Edge Computing). Tato technologie optimalizuje chod přístupové sítě. Za tímto vším stojí předpoklad, že v roce 2020 bude připojeno okolo 50 miliard mobilních zařízení. Pro srovnání v roce 2015 to je okolo 5 miliard zařízení. Všeobecně se tlačí na používání páté generace bezdrátových systémů a to hlavně sektorech jako jsou správy měst, energetika, zemědělství, zdravotnictví, ale i v běžných domácnostech. Aby bylo možné toto uvést v praxi, musí tyto technologie podporovat všechna zařízení. S tím jsou i úzce spjaté nároky na zařízení, která se mají do této sítě připojit. Jedna z vizí budoucnosti je inteligentní dům, který bude komunikovat pomocí aplikace 5G přímo s uživatelem o aktuálním stavu, aktuální spotřebě energií, o plánovaných údržbách nebo mu jenom připomene například nákup či zaplacení určitých položek. [11]

Kompletní vývoj mobilních sítí během jednotlivých let je popsán na obrázku 4. [6]



Obr. 2: Vývoj mobilních technologií [24]

### 1.4.2.8 Srovnání vlastností bezdrátových technologií

Tab. 2: Porovnání bezdrátových technologií část 1

IEEE technologie	IEEE standard	Max. přenosová rychlost Mb/s
Bluetooth	802.15.1	1
ZigBee	802.15.4	0,25
Wi-Fi	802.11.a b g n ac ad af ah ax	54
WiMAX	802.16	75
UWB	802.15.4a	0,11   0,85   6   8   27

Tab. 3: Porovnání bezdrátových technologií část 2

IEEE technologie	Kmitočtové pásmo [GHz]	Šířka pásma	Modulace
Bluetooth	2,4   2,4835	1	GFSK
ZigBee	0,868   0,915   2,4	0,3   0,6   2	BPSK (plus ASK), Q-QPSK
Wi-Fi	2,4   5	22	BPSK, QPSK, COFDM, CCK, M-QAM
WiMAX	2 až 11	1,25   5   10   20	QAM
UWB	3 až 7	500	BPSK, QPSK

### 1.4.2.9 Porovnání mobilních sítí

Tab. 4: Porovnání mobilních sítí

Generace	Přístupová technologie	Přenosová rychlost [Mbit/s]	Kmitočtové pásmo [MHz]	Šířka pásma [MHz]
1 G	AMPS, FDMA	0,0024	800	0,03
2 G	GSM, TDMA, CDMA	0,01	850   900   1800   1900	0,2 - 1,25
2,5 G	Obecná rádiová paketová služba	0,05	850   900   1800   1900	0,2
	EDGE	2,3		
3 G	WCDMA, UMTS	0,384	800   850   900   1800   1900   2100	5
	CDMA			1,25
4 G	LTE-A, OFDMA/SC-FDMA	DL 3000 Mbit/s, UL 1500 Mbit/s	1800   2600	1,4 - 20
	WiMAX, SOFDMA	100 - 200 Mbit/s	2300   2500   3500	3,5   5   7   10
	WiMAX			
5 G	BDMA, FBMC	10000 - 50000 Mbit/s	1800   2600 v budoucnu: 30000 - 300 000	60.000

## 1.5 Historie WLAN

Profesor Norman Abramson v roce 1970 dokázal sestavit první bezdrátovou počítačovou síť. Síť, kterou nazval ALOHAnet, nepoužívala telefonní linky, ale byla založená na použití levnějšího spojení pomocí radioamatérských stanic. Síť se skládala z centrálního počítače na ostrově Oahu a zbylých sedmi počítačů, které byly rozmístěny na čtyřech ostrovech, a komunikovaly s tímto centrálním počítačem. WLAN byly zpočátku velmi drahé a spíše byly určeny tam, kde se z nějakého důvodu, jako například z důvodu obtížného či nemožného použití kabeláže, nedala použít LAN. První tyto bezdrátové sítě používali proprietární protokoly a různá specifická řešení až do roku 1990 kdy normy tyto protokoly nahradily a vznikly různé verze IEEE 802.11, které ve svých produktech nesly označení Wi-Fi. Tento nový standard umožňuje použití přenosové rychlosti až 600 Mbit/s a to ve dvou frekvenčních pásmech 2,4 a 5 GHz. V dnešní době umí většina routerů na trhu pracovat jak v pásmu 2,4 GHz, tak v pásmu 5GHz. Vyjimku tvoří routery pohybující se v nižší cenové relaci. Tato možnost se nazývá dualband. To jim umožňuje v případě zaplnění pásma 2,4 GHz, které kromě Wi-Fi používají i mikrovlnné trouby, technologie Bluetooth, ZigBee použít i pásmo 5 GHz, které umožňuje připojení většího množství zařízení, která na daném prostoru sdílí síť. [25]

## 1.6 Bezdrátová technologie WLAN

Jedná se o bezdrátovou komunikaci standardu IEEE 802.11 ve WLAN (Wireless LAN) sítích. V dnešní době se hojně používá pro standardy IEEE 802.11 název Wi-Fi. Značení jednotlivých standardů navrhuje instituce IEEE, síťové standardy nesou označení 802. Pro Wi-Fi měly označení 802.11. Poté bylo přidáno označení pomocí latinských písmen, které značily přenosové rychlosti a v neposlední řadě frekvenční pásma, se kterými pracovaly. Wi-Fi alliance rozhodla o tom, že se budou standardy IEEE 802.11n, 802.11ac a 802.11ax přeznačovat a to tak, aby znázorňovaly jejich generace pomocí jedné číslovky. Jejich přechodní verze 802.11a, 802.11b a 802.11g si ponechají původní označení. Standard IEEE 802.11n se tak nově bude jmenovat Wi-Fi 4, standard IEEE 802.11ac se přejmenuje na Wi-Fi 6 nejnovější verze IEEE 802.11ax. Tento standard má nejvyšší datovou propustnost. Přenosová rychlost zde může dosahovat až hodnoty 11 Gbit/s, počítá také s lepším plánováním pro využití frekvenčního pásma v případě připojení většího množství zařízení. Počítá se i s lepším zabezpečením a to díky WPA3 (Wi-Fi Protected Access), která je plánovaná na rok 2020 a také počítá s nižšími nároky na energie na koncových zařízeních. Standard 802.11ax nově přejmenovaný na Wi-Fi 6 má 25%vyšší propustnost oproti modulaci 256-QAM u předchozí verze (Wi-Fi 5) a to díky tomu, že využívá modulaci 1024-QAM. Nově je zde možnost i duplexního provozu díky technologii MU-MIMO (Multiple-User Multiple-Input Multiple-Output), která u Wi-Fi 5 byla možná pouze u downlinku. Všechny tyto standardy využívají bezlicenční pásma od 2,4 do 5 GHz. [17]



## 2 SOUČASNÉ POŽADAVKY NA WLAN

Dříve se internet a bezdrátová technologie realizovala v rámci armády anebo univerzit v okruhu zasvěcených odborníků. Pro širokou veřejnost začaly být WLAN technologie dostupné již v letech 2002 až 2004 a to díky příchodu standard IEEE 802.11 n, dnes přejmenovaného na Wi-Fi 4, který znamenal velký posun oproti předchozím standardům a to hlavně díky přenosové rychlosti, která byla až 600 Mbit/s, šířka pásma mohla být od 2,4 do 5 GHz a šířka přenosového kanálu se mohla měnit z 20 až na 40 MHz. Dodnes se tento standard hojně využívá. [33]

### 2.2 Parametry WLAN sítí

#### 2.2.1 Přenosová rychlost

U přenosové rychlosti je použita jako základní jednotka 1 bit za sekundu. Dnes se používají její násobky od Kbit/s, Mbit/s až po hodnoty Gbit/s. Přenosová rychlost je počet přenesených informací za jednu sekundu (jednotku času). Někdy se využívá i jednotka v bajtech za sekundu. Dnes může být přenosová rychlost zjištěna pomocí různých testovacích portálů nebo se stahují určité soubory ze serveru ke klientovi. Druhý způsob, ale může být nepřesný a to kvůli pátevní konektivitě. Přenosová rychlost velice závisí na propustnosti do národního a mezinárodního uzlu. V těchto uzlech je ovlivněn provoz internetových služeb. Pak zde pro dostatečnou přenosovou rychlost musí být národní i mezinárodní konektivita. Nedostatečná mezinárodní konektivita se může projevit v rychlosti připojení nebo stahování informací ze serverů v zahraničí. [15]

#### 2.2.2 Antény

Se vznikem první antény je spojen koherer což byla skleněná trubička, která byla naplněná železnými pilinami, a která sloužila pro ověření přítomnosti elektromagnetických vln. Při dopadu této vlny se piliny zmagnetizovaly a v kontaktech začal protékat proud. Koherer původně sloužil jako detektor bleskových výbojů, dokud ho nepoužil Marconi, který ke svému experimentu vytvořil jiskřiště, využil anténu jako dlouhého drátu, který připojil na konec draka. Dalšími experimenty Marconi usoudil, že délka antény vůči délce vlny souvisí s vyzařováním antény. Za druhé světové války vývoj antén pokračoval dopředu. Díky novým rádiovým technikám byly nároky i na antény a proto

vznikly směrové antény. Dalším vývojem prošly také antény s parabolickým odražečem. Po válce došlo k vývoji polovodičů a vakuových součástek. Díky nim se mohlo vynalézt zařízení, které mohlo pracovat i s centimetrovými vlnami. Antény tak měly nové vyzařování. V době tohoto vývoje byla vynalezena šterbinová a trychtýřová anténa, které se využívaly v armádě a ve vesmírném programu. Během sedmdesátých a osmdesátých let došlo k zobecnění návrhu antén a to díky numerickým metodám, které řešili návrh určité antény. Dříve se používalo analytických metod, které byly o poznání složitější než ty numerické. Velký podíl na tom měl rozvoj výpočetní techniky. V tomto období byla vynalezena patch anténa a další její varianty. Dnešní antény jsou mnohopásmové a širokopásmové, dochází k jejich zmenšování a k automatickým návrhům. Rezonanční frekvence úzce souvisí s délkou antény. Tento jev se objeví při buzení antény daným signálem, kdy se napětí ze zdroje rozkmitá a díky tomu je vyzařování antény větší. Antény mají hodně rezonancí pro různé jejich frekvence. Tento fakt je použit v mnohopásmové aplikaci. Ohledně zisku je to tak, že anténa, která má vysoký zisk, směřuje vlnu úzkým směrem, zatímco anténa s nízkým ziskem je všesměrová. Tento zisk je pasivní veličina, protože výkon nepřidává sama anténa. Zisk může být jak kladný tak i záporný v závislosti na tom, jestli je některá elektromagnetická vlna nasměrována z jednoho směru více a z druhého směru méně. Účinnost antény se může vypočítat jako poměr mezi vyzářeným výkonem a výkonem na svorkách, anebo jako odpor záření k celkovému odporu, ve kterém jsou započítány i ztráty. Šířka pásma u antén značí rozsah frekvencí s tím, že rezonanční kmitočet ve většině případů bývá uprostřed rozsahu. Šířka pásma se u antén může zvětšit použitím širších dipolů a nebo upravou vstupní impedance. [8]

### **2.2.3 QoS, kvalita služby ve WLAN**

Ze začátku nebylo u WLAN zajištění kvality služeb QoS na spojové vrstvě součástí základních specifikací, jako tomu bylo u LAN. S postupem času a rozvojem přenosu videa v reálném čase a hlasu byla QoS u WLAN vyžadována. Bezdrátová síť je ale specifické prostředí, které má v mnoha ohledech jiné parametry než LAN síť. WLAN může ovlivňovat útlum, rušení i šum a to závisle na prostředí, čase vysílání a měnící se kapacitě kanálu. U QoS nezáleží na tom jak moc je daná síť rychlá.

Závisí zde na tom, jak zajistí přenos dat podle charakteristik, které souvisí se SLA (Service Level Agreement). K charakteristikám QoS se mohou zařadit koncová zpoždění,

jitter, což je kolísání zpoždění, ztráty různých paketů a v neposlední řadě šířka pásma, která souvisí s propustností.

Rozšíření EDCF (Enhanced Distribution Coordination Function) je prioritní pravděpodobnostní mechanismus pro přidělení šířky daného pásma a to na podstatě kategorií provozu. Pokud existuje stanice, která nepodporuje QoS, tak se bude automaticky řadit ke kategorii best effort. Stanice mohou jednotlivě vysílat pouze tehdy, pokud je médium volné, a to až po dané době čekání, která je stanovená kategorií provozu AIFS (Arbitration Interframe Space). Tato doba je pevně nastavena pro všechny přístupové kategorie s tím, že interval, po který se čeká, je doplněn náhodně dlouhým oknem sváru CW. CW pak brání kolizím paketů ze stejné kategorie. Existuje i složitější rezervační mechanismus než je QoS, který má v možnostech IEEE 802.11e a to HCCA – HCF (Controlled Channel Access).

QoS plánuje vysílací dobu, kdy jeden z provozů má možnost mít větší část kanálu. AP (Access Point) uděluje možnost vysílání a to pomocí osmi identifikátorů provozu. HCCA, která má nastavené parametry jako QoS, zajistí takové využití přenosového kanálu tak aby bylo efektivní a to hlavně u WLAN, které se používají pro přenos videí a hlasu. Zajistí to hlavně díky tomu, že odstraní ztrátové doby čekání. [3]

Zpoždění (delay) je definováno jako čas, který je potřebný k tomu, aby se paket dostal od zdroje do svého stanoveného cíle tedy k příjemci. Celkové zpoždění je složené z několika zpoždění, které nastávají při kódování, paketizaci, při přenosovém zpoždění, při čekání ve frontě než se paket odbaví a v neposlední řadě nastává zpoždění kvůli přepínání v síti. Kolísání zpoždění (Jitter) je čas, kdy pakety čekají ve vyrovnávacích pamětech a odbavovacích frontách, není vždy konstatní. Tento čas závisí na několika parametrech. Jedním z nich je architektura celé sítě a její aktivní prvky, které mají určité parametry. Dalším faktorem je i aktuální zátěž sítě. V krátkých frontách může docházet ke ztrátám paketů a to z toho důvodu, že se do fronty nevlezou, zatímco u dlouhých front dochází k pomalému zpracování, což má za následek vysoké zpoždění. Tyto situace jsou největším problémem pro hlasové služby, které jsou na toto nejvíce citlivé. Aby se tento problém vyskytoval co nejméně, používají se speciální vyrovnávací paměti. [46]

### 2.2.4 Výkon

Výkon související s dosahem je ovlivněn použitým frekvenčním pásmem, výkonem daného vysílače, citlivostí přijímače, ziskem a typem antény a v neposlední řadě způsobem modulace. Wi-Fi vysílače sice nevyzařují takové množství energie jako je tomu například u mobilních telefonů, ale tato vyzářená energie je mnohem vyšší než třeba u jiných bezdrátových technologií jako je Zigbee nebo Bluetooth. Evropská unie toto množství energie reguluje nařízeními a to na hodnotu 20 dBm což odpovídá 100 mW.[26]

### 2.2.5 Pořizovací cena

Wi-Fi router se dnes dá pořídit za cenu od necelých tří set korun až za cenu dvaceti a více tisíc. Existuje i několik stránek, které nabízí srovnání cen jednotlivých Wi-Fi routerů a to včetně recenzí o nich. K nejlevnějším routerům se řadí ty, které jsou od tří do šesti stovek. Některé routery mají pouze jednu anténu, příjem dat je u nich pomalý a ne všechny technologie jsou u nich podporovány. Výrobce může na obalu deklarovat rychlost 300 Mbit/s, což v reálném provozu nemusí být pravda, protože jeho rychlost se výrazně snižuje prostředím, v jakém se router nachází. Typické překážky jsou tlusté železobetonové zdi. Tyto Wi-Fi routery jsou určeny do malých bytů a chat a pro uživatele, kteří na ně nekladou vysoké nároky. Routery, které stojí do dvanácti set korun, jsou určeny pro uživatele, kteří mají větší plochy na pokrytí sítě, chtějí mít rychlejší připojení a menší výpadky. Typicky jde o domácnosti, kde se přenosová rychlost pohybuje okolo 300 Mbit/s. Tyto routery mají i více než dvě antény, takže se jejich signál může nasměrovat a tím zvýšit i dosah signálu. Jejich cena není tak vysoká a proto si je může dovolit široká veřejnost a jsou také nejvíce zastoupeny na trhu. Do necelých dvou tisíc korun jsou routery, které se dají použít i v restauracích, kavárnách i firmách a pro náročné uživatele v domácnostech. Tyto routery už mají vynikající parametry. Mají čtyři a více antén, výběr frekvenčního pásma, jsou kompatibilní s moderními funkcemi a jejich přenosová rychlost bývá větší než 500 Mbit/s. Mají také stabilní připojení. Jejich nevýhoda tkví ve větších rozměrech a ve vyšší ceně oproti předchozím Wi-Fi routerům. Nejlepší Wi-Fi routery s největším výkonem stojí přes deset a více tisíc. V běžné domácnosti se neobjevují, ale využívají je například větší firmy s velkou četností připojených zařízení, anebo hráči, kteří chtějí mít plynulý a rychlý přenos pro hraní online

her a vysílání online přenosu na internet. Pro běžného uživatele jsou tato zařízení jak k provozu zbytečná, tak hlavně cenově méně dostupná. [16]

## 2.3 Standardy WLAN sítí

Standard IEEE 802.11 byl poprvé uveden v roce 1997. Byl používán jako možnost k bezdrátovému propojení. Tuto možnost využívají WLAN sítě, které pomocí skupiny standardů IEEE 802.11 mají nadefinované schéma bezdrátového spojení a první i druhou vrstvu modelu ISO/OSI. To znamená, že tato skupina standardů udává specifikace pro fyzickou vrstvu, pro vrstvu linkovou udává jen část. Tyto standardy vyvíjí a spravuje společnost IEEE (Institute of Electrical and Electronics Engineers). V tomto institutu spravuje jedenáctá skupina komise pro standardy standard IEEE 802.11. Zde se vyvíjí řešení pro LAN - lokální a MAN – metropolitní sítě. V krátké době se vytvořilo relativně mnoho standardů pro fyzickou vrstvu IEEE 802.11. Označení těchto standardů se rozlišovalo v příponě pomocí latinských písmen. [10]

### 2.3.1 IEEE 802.11 (legacy) – 1-2 Mbps

Byl uveden v roce 1997 jako první standard pro bezdrátové sítě a definoval fyzickou vrstvu s využitím pro pásmo 2,4 GHz. Jeho maximální přenosová rychlost byla od 1 Mbit/s až do 2 Mbit/s a jeden z jeho kanálů zabíral šířku 22 MHz. [10] V praxi se už nevyužívá, protože byl vyměněn za lépe vyhovující verze. V praxi to ovšem pomohlo k nastavení a zavedení určitých principů pro bezdrátové sítě, které se na tomto základu používají dodnes. Tento standard někdy i nazývaný 802.11 legacy má tři možnosti jak posílat data na fyzické vrstvě. Jedna z možností je přenos dat díky rádiovým vlnám pomocí FHSS - frekvenčních skoků anebo pomocí metody DSSS – přímého rozprostření spektra a to vše v pásmu 2,4 GHz. Třetí možnost je přenos díky infračervenému záření, tento přenos nemá konkrétní implementaci. Tento standard řeší i problémy ohledně přístupu k médiu. Používá CSMA/CA, což je metoda na vyhýbání kolizí s vícenásobným přístupem k médiu. Důvodem použití zrovna této metody je nemožnost detekovat kolize. Média musejí čekat náhodně zvolený interval, než odešlou každý rámeček. To je podstatný rozdíl oproti metodě CSMA/CD kdy médium začíná čekat pouze, když nastane kolize.[9]

### 2.3.2 802.11a – 1,5-54 Mbps

O dva roky po uvedení standardu IEEE 802.11 legacy se v roce 1999 představil standard IEEE 802.11a, který už uměl i využít pásmo 5 GHz a šířka jednoho z jeho kanálů byla 20 MHz. Několika násobně se zvýšila i přenosová rychlost a to na hodnotu 54 Mbit/s.

K dosažení takovéto rychlosti se použila možnost širokopásmové modulační techniky ortogonálního multiplexu s OFDM – frekvenčním dělením. Tato zvolená technika se i nadále využívá ve většině standardů. [10] Šířka nově využitého pásma 5 GHz přinesla hlavní výhodu a to tu, že zde byla menší pravděpodobnost rušení než v pásmu 2,4 GHz, ve kterém je nejenom WLAN, ale i Bluetooth, nebo mikrovlnné trouby. Další z výhod je množství dohromady dvanácti kanálů, které se navzájem nepřekrývají. V pásmu 2,4 GHz jsou pouze tři nepřekrývající se kanály. Ovšem jsou zde i výrazné nevýhody jako například nekompatibilita se staršími zařízeními, které využívají pouze pásmo 2,4 GHz, nižší dosah kvůli vyšší frekvenci, která hůře proniká prostředím než jak je tomu u frekvence 2,4 GHz. [9]

### **2.3.3 802.11b – 11 Mbps**

Ve stejném roce jako vznikl standard IEEE 802.11a vznikl i standard 802.11b, který pracuje ve stejném pásmu a má i tu samou šířku kanálu jako 802.11a. Pro přenos využívá DSSS modulaci na fyzické vrstvě. [10] Tento standard byl spíše takovým pokračováním standardu 802.11a než, že by přinesl něco převratného. Co bylo u tohoto standardu nové, je interoperabilita se zastaralými médii, kterou doplňuje pro 802.11a. [9]

### **2.3.4 802.11g – 54 Mbps**

Standard 802.11g byl uveden v roce 2003, má šířku kanálu 20 MHz s maximální přenosovou rychlostí 54 Mbit/s a pracuje v pásmu 2,4 GHz. Fyzická vrstva je založena jak na DSSS tak i na OFDM. [10] Díky DSSS modulaci je zde možnost připojení starší elektroniky. Je tedy velice podobný standardu 802.11a s možnostmi 802.11b. Jedna z nevýhod, která zde zůstává, je určitá pravděpodobnost rušení v pásmu 2,4 GHz z důvodů přeplnění tohoto pásma. [9]

### **2.3.5 802.11n – 300 Mbps**

Tento standard vyšel o šest let později než 802.11g a to v roce 2009. 802.11n výrazně posunul technologii WLAN dopředu. Jedna z jeho výhod je použití pásma 2,4 GHz tak i pásma 5 GHz, šířka kanálu může být 20 MHz anebo 40 MHz. Na fyzické vrstvě se používá modulační technika OFDM a nově je zde přenosová rychlost posunuta až na 300Mbit/s. Novinkou je zde i technologie MIMO (Multiple-Input Multiple-Output). Ta dává možnost využít v rádiovém kanálu více antén, které mohly vytvořit více datových

toků ve stejném pásmu a díky tomu se může dosáhnout i větší přenosové rychlosti. [10] Tento standard pro bezdrátové technologie byl jako první schopen konkurence před technologií Fast Ethernet. Nevýhodou bylo, že kvůli možnosti rozšíření šířky pásma z 20 na 40 MHz nastaly problémy s interferencí v pásmu 2,4 GHz a proto by se tato možnost měla využívat pouze tehdy, pokud bude jisté, že nebude ovlivňovat žádné další bezdrátové technologie ve svém okolí jako je Zigbee nebo Bluetooth. Tato možnost rozšíření pásma je proto pro 5 GHz pásmo omezena. [9]

### **2.3.6 802.11ac – 6,933 Gbps**

Roku 2013 se vydal standard 802.11ac, který navazuje na předešlý standard 802.11n, který znamenal to, že se na bezdrátové síti začali klást čím dál větší požadavky a nároky. [10] Tento nový standard rozšiřuje šířku pásma kanálu za účelem ještě vyšší přenosové rychlosti. Konkrétně ho rozšiřuje z možnosti 20 a 40 MHz na možnost využít 80 až 160 MHz. Proto tento standard využívá šířku pásma jenom 5 GHz. Jsou zde i větší možnosti technologie MIMO, která je zde rozšířena o možnost navýšení přenosů ze současných čtyř na osm a také je zde možnost tyto přenosy vysílat na více koncových zařízení. [9] Fyzická vrstva je založena stejně jak u předešlých standardů na modulační technice OFDM a maximální přenosová rychlost zde může vyšplhat až na hodnotu 6,933 Gb/s. V dnešní době je tento standard nejrozšířenější. [10]

### **2.3.7 802.11ad – 6,756 Gbps**

Tento standard byl uveden o rok dříve než standard 802.11ac a to v roce 2012. Od všech standardů se lišil v šířce použitého pásma, která je 60 GHz. Tím se dá rozšířit i šířka pásma kanálu až na hodnotu 2160 MHz. Nevýhoda u tohoto standardu je možnost použití pouze na menší vzdálenosti, než je tomu třeba u standardů, které využívají pásmo 2,4 GHz. S použitím vyšší šířky pásma dochází i rychleji k útlumu signálu průchodem daného prostředí. Teoreticky se zde dá využít přenosové rychlosti až 6,756 Gbit/s. OFDM je opět využito na fyzické vrstvě tak jako tomu je u předchozích standardů a navíc pracuje se SC - Single Carrier rozprostřeným spektrem. [10]



### 2.3.8 802.11af a 802.11ah

Tyto standardy jsou zatím nejnovější z celé této skupiny standardů. 802.11af je z roku 2014 a 802.11ah je z roku 2016. Hlavní jejich cíl je dosažení bezdrátového přenosu na co možná největší vzdálenost a proto využívá šířku pásma pod 1 GHz kde, ale nemůže využít velkou šířku pásma kanálu a nemůže proto dosahovat velkých rychlostí přenosu jako je tomu u předešlých standardů. Vzdálenost pro bezdrátový přenos může dosáhnout na hodnotu až stovky metrů. Fyzická vrstva je zde opět postavena stejně jako u předešlých standardů a to na modulační technice OFDM. [10]

## 2.4 Tabulka srovnání jednotlivých standardů

Tab. 5: Srovnání standardů 802.11 [30]

IEEE standard	rok založení standardu	kmitočtové pásmo [GHz]	šířka pásma 1. kanálu [MHz]	max. přenosová rychlost [Mbit/s]	modulace
802.11	1997	2,4	22	2	DSSS, FHSS
802.11a	1999	5	20	54	OFDM
802.11b	1999	2,4	22	11	DSSS
802.11g	2003	2,4	20	54	DSSS, OFDM
802.11n	2009	2,4 nebo 5	20   40	600	OFDM
802.11ac	2013	5	20   40   80   160	6933	OFDM
802.11ad	2012	60	2160	6756	OFDM
802.11af	2014	0,54 až 0,79	6   7   8	26,7	OFDM
802.11ah	2016	0,9	1   2   4   8   16	40	OFDM
802.11ax	2019	2,4 nebo 5	20   40   80   160	9607,8	OFDM, OFDMA

## 2.5 Zabezpečení WLAN

Veřejná WLAN, kterou má v dnešní době téměř každá kavárna nebo restaurace je zdarma nebo za malý poplatek. Je zde ale riziko odposlouchávání uživatelské komunikace. Útočníci se takto mohou dostat do zabezpečeného přístupu podnikové sítě nebo k citlivým datům uživatele. [5]

WLAN jsou oproti LAN náchylné na útoky. Tyto útoky se dají rozdělit na dvě základní kategorie a to pasivní a aktivní. Do pasivních útoků můžeme zařadit různé odposlechy a v neposlední řadě analýzu provozu sítě. Tyto pasivní útoky jsou na první pohled nezjistitelné. Útočník nijak neovlivňuje chod sítě ani nemění data uživatele. Oproti tomu aktivní útoky jsou například modifikování zpráv, falšování uživatelské identity, odmítání

různých druhů služeb například DoS a zásahy do dat uživatele. Tyto útoky jsou nebezpečné pro uchovávání citlivých dat a v bankovním systému.

Možnosti zabezpečení proti možným útokům je umožněno použitím: [5]

### **2.5.1 SSID (Service Set Identifier)**

je identifikátor používaný pro značení prvků systému WLAN. Je dlouhý 0-32 oktetů. Přístupový bod v základním nastavení vysílá SSID opakovaně několik sekund a to pomocí zprávy beacon z toho důvodu, aby o něm uživatelé věděli. Přístupový bod nemusí pravidelně vysílat beacon a SSID, ale i přesto může útočník snadno tento přístupový bod zjistit. Útočník může poslat falešný požadavek na odpojení aktivní stanice. Stanice je pak nucena znovu se připojit pomocí zpráv Probe a Associate a tak může útočník odhalit pomocí SSID skrytou WLAN síť. Proti možným útokům je doporučené SSID měnit, nevysílat beacon s SSID a změnit základní nastavení SSID na hodnotu, která je pro útočníka hůř zjistitelná. [5]

### **2.5.2 ESSID (Extended Service Set Identification)**

je naprogramovaná hodnota do přístupového bodu pro ověření přístupu do sítě. ESSID oproti SSID opakovaně nevysílá a proto o něj mohou požádat pouze autorizované stanice, které hodnotu ESSID znají. Tato síť je označována za uzavřenou. [5]

### **2.5.3 Šifrování WEP (Wired Equivalent Privacy)**

je algoritmus, který je založen na klíči o velikosti 10 nebo 26 hexadecimálních znacích. WEP byl původně navržen pro docílení větší bezpečnosti komunikace v bezdrátové síti, takové jaké je v LAN sítích. Bohužel se toho nedocílilo. U WEPu se používá symetrický postup. To znamená, že na šifrování i dešifrování je použit jeden algoritmus a jeden klíč. WEP může případný útočník narušit jak odposlechem, tak i krádeží koncového zařízení, které obsahuje příslušnou WiFi kartu. Pokud dojde k narušení prolomením klíče nebo krádeží, musí se na všech zařízeních, která používají stejný klíč, tento klíč obměnit. [5]

### **2.5.4 Šifrování WPA (Wi-Fi Protected Access)**

vznikl v roce 2002, aby řešil slabiny šifrování WEP do doby, než se schválí doplnění bezpečnostní normy 802.11i. WPA používá šifrovací mechanismus, který je stejný jako v případě WEP. Proto se vylepšení WPA oproti WEP týkalo spíše

softwarových/firmwareových změn. WPA nabízí autentizaci pro firemní sítě, tak i pro domácí sítě. WPA poskytuje snadnou implementaci s PSK. Nevýhodou je však případná nemožnost dovybavení starších produktů šifrováním WPA. [5]

### **2.5.5 Šifrování WPA2**

vznikl v roce 2004 jako nový produkt Wi-Fi Alliance. Certifikace WPA2 nabízí možnost rozdělení pro domácí, tak i pro firemní sítě. Tato možnost autentizace je stejná jako při šifrování WPA.

Pokročilejší šifrování je možné díky implementaci povinného protokolu CCMP (Counter mode Cipher block chaining Message authentication code Protocol) a AES (Advanced Encryption Standard). [5]

### **2.5.6 Šifrování WPA3**

je nejnovější generace pro zabezpečení Wi-Fi. Na rozdíl od starší WPA2, tak WPA3 zjednodušuje zabezpečení Wi-Fi, má dalekosáhlé ověřování a zakazuje použití starších protokolů, které jsou rizikové. Tato generace se zaměřuje jak na osobní využití, tak na využití pro firmy. WPA3-personal dodává svým uživatelům vyšší zabezpečení před odhadem hesla a WPA3-enterprise poskytuje vyšší zabezpečení pro datové sítě. [36] Tato nová verze má složitější ověřování a šifrování je zde silnější, než u předešlé WPA2. Používá 192 bitové šifrování, které je založené na AES-256 a SHA-384, vyřazuje zastaralé protokoly a prosazuje použití PMF (protected management frames). [26] WPA3- personal, jak už z názvu vyplývá, se zaměřuje na uživatele a na jeho požadavky pro zabezpečení hesla. Když si uživatel zvolí heslo, které je slabé tj. nesplňuje délku, počet písmen a čísel, tak WPA3 personal pomocí SAE - simultánní autentizace rovných zaměnní předsdílený klíč PSK. Tento způsob zabezpečení odolává útokům offline slovníku pomocí kterého se může určit síťové heslo. Pro uživatele to má pozitivní dopad v tom, že si může zvolit heslo, které si dobře pamatuje a u kterého se nemusí bát, že s ním bude mít problémy ohledně jeho síly zabezpečení. Pro vládní instituce, velké podniky a finanční sektor je výhodné používat WPA3- enterprise, která má na výběr 192 bitové protokoly a používá kryptografické nástroje, kterými chrání citlivá data. K ověření šifrování využívá protocol GCMP-256 Galois/Counter Mode, který má 256 bitů. Pro odvizování a potvrzování klíče využívá HMAC, což je 384 bitový režim pro ověřování tvz. hash zpráv založený na algoritmu secure hash algorithm. Se stanovením klíče a jeho

ověřením pracuje s ECDH, což je výměna Diffie-Hellman eliptické křivky a digitální podpis ověřuje díky 384 bitové eliptické křivce. Galois Message- BIP-GMAC-256 je 256 bitový protokol pomocí kterého se ověřuje integrita vysílání a vícesměrové vysílání.

[36]

## **2.6 Použití WLAN ve firmách**

WLAN použité ve firmách jsou prodloužením pevné LAN. Nejčastěji se jedná o Ethernet. Tato WLAN musí plnit stejné funkce jako síť pevná. Jedná se především o funkce managementu, zabezpečení a škálovatelnosti. [5] Pro firmy je mnohem praktičtější a cenově výhodnější zavedení bezdrátové komunikace. Bezdrátové technologie v průmyslové práci umožňují inovace pro přenosné počítače, tablety a mobilní telefony. Firmy se mohou při použití bezdrátové technologie připojit do databáze a informace vyhledávat mnohem snadněji a rychleji. Podniková WLAN má mnohem větší spolehlivost i výkonnost než WLAN použitá v domácnostech. [34]

## **2.7 Použití WLAN v domácnostech**

Možnost efektivního propojení všech zařízení v domácnosti do jedné funkční sítě. Dnes se nepropojuje jenom výpočetní technika, spotřební elektronika ale i domácí spotřebiče a elektronické systémy. To všechno se dnes může připojit k WLAN. [5] WLAN šetří peníze na použité kabeláži, kde by cena výrazně stoupla. Je také mnohem jednodušší na fyzickou instalaci. Bezdrátové sítě požadují jeden AP, který je připojený přes router k internetu. Bez použití bezdrátové technologie by nebylo možné sdílet tiskárny, skenery a vysokorychlostní internet. [34]

## **3 TEORETICKÝ NÁVRH MĚŘENÍ**

V programu Riverbed je realizováno zapojení sítě, tak aby docházelo k rušení v pásmu 2,4 GHz. Toto rušení je docíleno výběrem vhodného vysílacího výkonu, kanálu a pásma. Velkou roli v sestavení zapojení hraje i standard a přenosová rychlost. Toto zapojení v programu Riverbed je sestavené pro parametry routerů Mercusys, které pracují v pásmu 2,4 GHz.

### **3.1 Rušení WLAN sítě**

Rušení WLAN sítě může být způsobeno jak vnějšími vlivy, tak i zahlcením jednotlivých kanálů během spuštění přístupových bodů. Možné je také rušení způsobené větším množstvím přístupových bodů v oblasti.

Pro minimalizaci poruch se používá CSMA/CA protokol. Před vysíláním zařízení poslouchá, zda na daném kanálu neprobíhá jiná komunikace. [26]

### **3.2 Použité programy pro realizaci laboratorních úloh**

#### **3.2.1 Riverbed**

Firma Riverbed vytvořila program Riverbed Modeler Academic Edition 17.5, který je dostupný pro školy, tak i pro jednotlivé studenty, kteří si ho mohou doma na svém počítači nainstalovat a dále ho používat. Studenti si v tomto programu mohou vyzkoušet vytvořit vlastní síť se všemi základními pojmy, síťovými protokoly a řízení reálných sítí a tak pochopit i základní pojmy. Tento program studentovi umožňuje navrhnout si vlastní síť, u které může analyzovat provoz při nejrozumnějších situacích a jejich následné řešení. Mohou si zde i vyzkoušet mechanismy síťových technologií a síťových protokolů včetně používání aktivních a pasivních prvků sítě jako jsou rozbočovače, směrovače, přepínače, servery a možnost přidání jednotlivých klientů. [14]

#### **3.2.2 Iperf3**

Program Iperf3 slouží k ověření komunikačních parametrů drátových či bezdrátových technologií. Program Iperf3 je volně stažitelný a dostupný na webových stránkách <https://iperf.fr/>. Je vhodný na testování a ladění parametrů přenosu. Používá protokoly

TCP, UDP, STCP s využitím IPv4 a IPv6. Po skončení testování zobrazí parametry (šířku pásma, ztrátu paketů, časový interval, přenosovou rychlost). Program Iperf3 vyvíjela Národní laboratoř ESnet/Lawrence Berkeley. Funkce Iperf3 souvisí s výběrem jednotlivých protokolů. Pro TCP protokol je možné v programu IPerf3 změřit šířku pásma, velikost MSS/MTU nebo velikost TCP Window. Při výběru protokolu UDP je možné změřit šířku pásma, ztrátu paketů, jitter. Za jednu z výhod je možnost využití parametru  $-t$  během testování. Test pak může běžet libovolně zvolený časový úsek. Také je možné hodnoty z programu převést do formátu.xls, což umožňuje snadnější manipulaci s hodnotami. [52]

### **3.2.3 Scapy**

Scapy je program psaný v programovacím jazyce Python. Program Scapy je interaktivní výkonný program, který manipuluje s pakety (odesílá je a přijímá ve formě odpovědí). Má také schopnost, která umožňuje snímání, skenování nebo útočení na síť. Velice často nahrazuje hping, arpspoof, arp-sk, arping, p0f a dokonce i některé části Nmap, tcpdump a tshark. Pro začátečníka v pythonu se doporučuje projít tutorialy, které uživatele seznámí se základními příkazy, které se v programu mohou vyskytovat. Program Scapy lze propojit s programem Wireshark. Což umožňuje lepší možnosti pro testování sítě. Je také volně stažitelný a dostupný na webových stránkách programu. [53]

### **3.2.4 Wifijammer**

Tento skript psaný v jazyce python umí zahlcovat, deautorizovat a zpomalovat WiFi klienty a ostatní přístupové body, které jsou v dosahu. Pro jeho funkčnost je nutné nainstalovat program python, nebo python-scapy. Pro účinnost je zde také vyžadována externí WiFi karta. Tato karta umožní programu wifijammer na jedné síti naslouchat a na druhé ji zahlcovat. Program je velice jednoduchý na instalaci. Není vyžadována zkušenost s jazykem python. Návod, který je k tomuto programu k dispozici na internetu je přehledný a lehce srozumitelný. [54]

### 3.3 Předpokládaný závěr

Při softwarové realizaci laboratorní úlohy Vzájemné ovlivnění WLAN sítí je znatelné rušení mezi pásmem 2,4 GHz. Toto rušení je způsobeno působením dalších zařízení v okolí Wi-Fi routeru ve frekvenčním pásmu 2,4 GHz. Tím, že je frekvenční pásmo 2,4 GHz nelicencované a tudíž není zpoplatněné, tak v něm komunikuje spousta dalších zařízení. Mohou to být například mikrovlnné trouby, ledničky, dětské chůvičky, bezdrátové reproduktory, telephony a fotoaparáty. Nejčastěji je však rušení způsobeno nárustem Wi-Fi sítí v okolí. Tyto Wi-Fi sítě se tak doslova perou o své místo ve frekvenčním pásmu 2,4 GHz. Dotčená jsou převážně sídliště, popřípadě satelitní zástavby. Antény, které jsou součástí Wi-Fi routeru také značně toto rušení ovlivňují. Antény sice umožňují vysílání do všech směrů, ale také ze všech směrů signál přijímají. Značné zpomalení rychlosti Wi-Fi routeru způsobuje neustálé zpracování cizích Wi-Fi signálů. Aby nedocházelo k rušení, musel by být každý Wi-Fi router nastaven na jiný kanál anebo pevným připojením pomocí kabelu. Frekvenční pásmo 5 GHz sice není zahlcené tak jako frekvenční pásmo 2,4 GHz, ale v budoucnu je možné, že se zaplní i toto pásmo. Důležité je také vzít v potaz, že i místo na kterém je router umístěn hraje velkou roli v oblasti rušení. Rušení totiž mohou způsobovat i překážky, jako je nábytek či stěny. Pokud nejde navázat spojení, dochází ke ztrátě datagramů anebo pokud se zvětšuje zpoždění při přenosu, pak dochází k jevu zvanému zahlcení. Zahlcení je patrné nejvíce v pásmu 2,4 GHz, který trpí na rušení z jiných zařízení. Kvalita přenosu signálu je ovlivněna vzdáleností. Za rozumné, se dají považovat hodnoty signálu -45dB a -70dB. Na kvalitu přenosu mají také vliv překážky v blízkosti Wi-Fi routeru. Správné natočení antén má také vliv na kvalitu přenosu signálu. Pootočení jedné antény může způsobit znefunkčnění signálu. Běžně dostupné Wi-Fi routery se pohybují ve frekvenčních pásmech 2,4 GHz a 5 GHz. Za výhody v pásmu 2,4 GHz lze považovat dosah sítě, kdy si router lépe poradí s překážkami, jako jsou například zdi. Pásmo 2,4 GHz také lépe podporuje více zařízení v daném pásmu. Pásmo 2,4 GHz má oproti 5 GHz nevýhody, což se menší přenosové rychlosti týče. Další nevýhodou pásma 2,4 GHz je větší zahlcení provozu sítě než u pásma 5 GHz. Zařízení v domácnostech využívají toto pásmo pro svůj provoz. Technologie Bluetooth využívá také pásmo 2,4 GHz a proto při připojení bezdrátového telefonu pomocí technologie Bluetooth může značně ovlivnit kvalitu signálu Wi-Fi routeru. Výhody 5 GHz pásma jsou menší zahlcení kanálů, což souvisí s



jeho větší propustností a jejich vzájemné nepřekrývání. Za nevýhody lze považovat kratší dosah sítě. 5 GHz pásmo je více pohlcováno překážkami. Pásmo GHz nepoužívá tolik zařízení jako pásmo 2,4 GHz. Při prohlížení webových stránek, psaní emailů je dostačující pásmo 2,4 GHz, ale pro streamování filmů, které spotřebovává více objemu zařízení, je lepší využít pásmo 5GHz. Kvalitnější Wi-Fi routery se pohybují v řádech 1500 Kč a výš. Tyto routery se však používají spíše ve firmách. Pro běžné uživatele je využití těchto routerů zbytečné. Pro použití v domácnostech jsou dostačující Wi-Fi routery v cenové relaci do 500 Kč.

## 4 LABORATORNÍ ÚLOHY

V části 4 je popsáno softwarové zapojení laboratorní úlohy v program Riverbed a hardwarové zapojení laboratorní úlohy s využitím RPi 3, RPi Zero, RPi 4 a programu Iperf3. Softwarového zapojení úlohy, konfigurace jednotlivých zařízení použitých při měření, blokové schéma zapojení, přínos měření pro studenty a závěr je součástí první laboratorní úlohy. Hardwarové zapojení, konfigurace WiFi routerů, Konfigurace RPi 3, RPi Zero a RPi 4, ověření parametrů přenosu s využitím program Iperf3, rušení WiFi routerů pomocí program Scapy, zhodnocení a přínos pro studenty, grafy a Závěr jsou součástí druhé laboratorní úlohy. V přílohách jsou pak blíže popsány manuály pro vyučující, manuály pro studenty, vyhodnocení laboratorních úloh, ke kterým by studenti měli dojít a grafy, které studenti vloží do svého protokolu, jsou taktéž součástí přílohy.

### 4.1 Vypracování laboratorních úloh

Vhodný výběr programu je první bod pro vypracování laboratorní úlohy. Vzájemné ovlivnění WLAN sítí v pásmu 2,4 GHz a 5 GHz. Program Riverbed umožňuje vytvoření vlastních sítí, síťových protokolů a jejich řízení a konfiguraci. V programu Iperf3 studenti ověří základní parametry přenosu standardů IEEE 802.11 b a IEEE 802.11 n pro routery Mercusys, Netis, TP-Link a Asus. Sestaví přehledné tabulky a grafy. V programu Scapy pak využijí RPi 4 (Client/wifijammer) jako útočníka, který bude rušit přenos mezi RPi Zero (Client) a RPi 3 (Server). Pochopení analýzy provozu sítě při různých situacích a vlastní návrh řešení je to, co by si měl každý student vyzkoušet.

## 4.2 Semestrální laboratorní úloha – 1. Laboratorní úloha

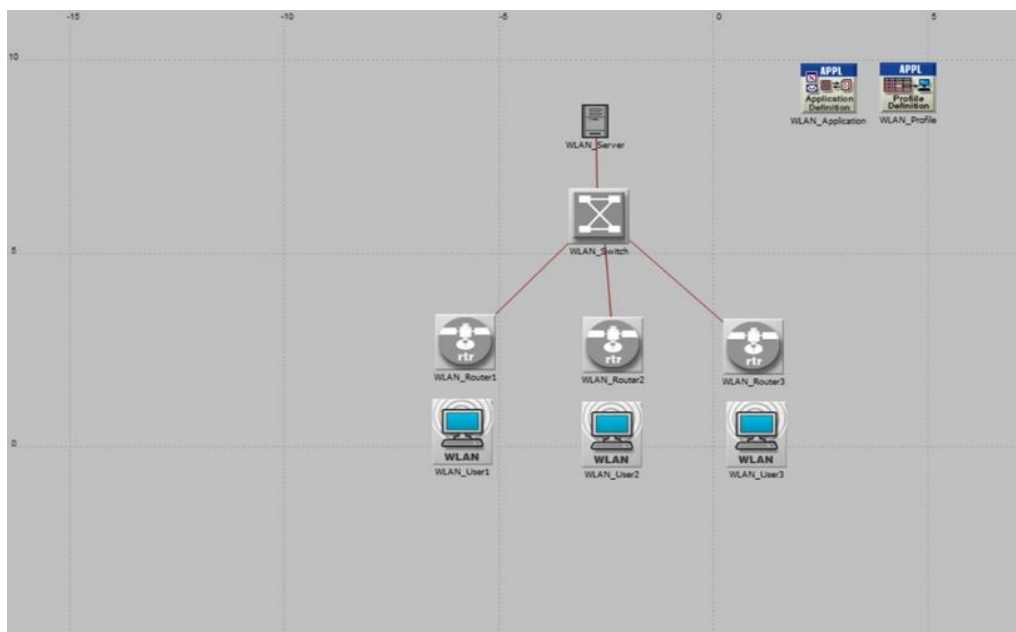
Postup Vypracování laboratorní úlohy v programu Riverbed

### 1) Založení projektu a práce s Object Palette Tree

Pro zobrazení vlivu rušení WLAN sítí je nutné spustit program Riverbed. Program Riverbed umístěný na ploše spustíme. Nejprve je nutné napamovat výchozí adresář, kam se má výsledný soubor uložit. V položce File => Manage model files => Add model directory. V novém okně se přepne na záložku Plocha (desktop). Zde v dokumentech => downloads => Riverbed project. Složku označit a potvrdit tlačítkem Ok. V okně Confirm model directory označit možnost Make this the default directory a potvrdit Ok. Pokud program projekt nedovolí uložit, je to způsobeno tím, že již projekt stejného názvu existuje a je nutné jej pozměnit. V záložce File => New => Enter Name se projekt pojmenuje jako WLAN\_Rušení a scénář (scenario) se pojmenuje Rušení. Dále se klikne na Ok a zvolené nastavení se potvrdí. Dále se zobrazí dialog Initial Topology, kde se zvolí Create empty scenario. Vše se potvrdí tlačítkem NEXT. V dialogu Choose network scale se zvolí možnost Campus, vše ostatní je ponecháno beze změny. V dialogu Specify Size se změni nastavení X span: 20, Y span: 20, Units: Meters. Vše se potvrdí tlačítkem NEXT. V dialogu Select Technologies se zvolí wireless\_lan a wireless\_lan\_adv. Vše se potvrdí tlačítkem NEXT. V dialogu Review se zkontrolují vybrané parametry a potvrdí se tlačítkem FINISH. Pro zapojení je nutné zvolit vhodné prvky, na kterých se postupně nastaví jednotlivé parametry. Z palety Object Palette Tree se vybere 3x wlan2\_ethernet\_router\_adv Fixed Node, které se rozmístí na plochu do tzv. trojúhelníku. Z palety Object Palette Tree dále vybereme přepínač ethernet16\_switch Fixed Node, který se umístí pod vybrané wlan2\_ethernet\_router\_adv. Dále se zvolí ethernet\_server Fixed Node a umístí se nad routery. Dále se vyberou 3x wlan\_wkstn\_adv Fixed Node, které se umístí pod routery. Každou stanici je nutné umístit pod vybraný router. Komponenty ethernet\_server a ethernet16\_switch jsou propojeny linkou 100BaseT k jednotlivým routerům. Propojení by mělo správně začínat od serveru k přepínači a tedy od komponenty ethernet\_server ke komponentě ethernet16\_switch. Dále by se mělo správně propojovat od routeru k přepínači. Správné propojení by mělo vypadat takto: wlan2\_ethernet\_router\_adv => ethernet16\_switch. Totéž je nutné udělat pro všechny routery v zapojení úlohy. Nakonec je důležité vybrat z palety Application

Config a Profile Config a umístit je v blízkosti serveru. Pojmenování jednotlivých komponent je vidět na obrázku 1.

Pojmenování se provádí pravým kliknutím na vybranou komponentu a zvolením Set Name.



Obr. 3: Sestavení úlohy

## **2) Konfigurace všech komponentů**

Konfigurace jednotlivých zařízení umožní nastavit parametry, jako je standard 802.11g a přenosovou rychlost 54 Mbit/s. Kliknutím pravým tlačítkem na komponentu wlan2\_ethernet\_router\_adv pojmenovanou jako WLAN\_Router1 se zobrazí lišta s možnostmi. Pro nastavení všech důležitých parametrů je důležité vybrat Edit Attributes. Zde se zobrazí jednotlivá nastavení pro router WLAN\_Router1. Po srolování možností téměř na konec pod System Information se nachází lišta Wireless LAN. Po rozkliknutí se zobrazí Wireless LAN Parameters, kde se nastaví hodnota BSS Identifier na 1. Nastavení se potvrdí tlačítkem Ok. Totéž se provede pro WLAN\_Router2, kde se ale nastaví hodnota BSS Identifier na 2. A u WLAN\_Router3 se tato hodnota nastaví na 3. Po nastavení jednotlivých routerů se nastaví parametry pro wlan\_wkstn\_adv. Opět se pravým klikne na vybranou komponentu workstation, pojmenovanou jako WLAN\_User1 a zobrazí se lišta Edit Attributes. V položce Wireless LAN Parameters zvolíme hodnotu BSS Identifier tak, aby odpovídala routeru nad danou stanicí. Pro WLAN\_User1 tato hodnota bude nastavená na 1. Pro WLAN\_User2 bude nastavená na hodnotu 2 a pro WLAN\_User3 na hodnotu 3. V horní liště, v záložce Protocols, je možné nastavit standard a přenosovou rychlost pro jednotlivé routery. V liště je nutné zvolit možnost Wireless LAN => Configure PHY and Data Rate. Objeví se lišta, ve které se dá jednoduše zvolit standard a přenosová rychlost. Pro vzájemné ovlivnění WLAN sítí je vhodné vybrat standard, který podporuje pásmo 2,4 GHz a nejnižší možnou přenosovou rychlost, kterou standard nabízí. Standard 802.11g pracuje v pásmu 2,4 GHz a nabízí přenosovou rychlost 54 Mbit/s. A proto je pro tuhle úlohu nejvhodnější. Program Riverbed automaticky nabízí tento standard a není tedy nutné nic měnit. Potvrdí se výběr tlačítkem Ok. Dále je potřeba nakonfigurovat Application Config a Profile Config. Pravým kliknutím na komponentu komponentu pojmenovanou jako WLAN\_Application se zobrazí lišta, ve které se zvolí Edit Attributes. V položce Application Definitions je třeba zvolit hodnotu Number of Rows na Default. Konfigurace komponenty WLAN\_Profile se provede kliknutím pravým na tuto komponentu, kde se zobrazí lišta, ve které se zvolí Edit Attributes. V záložce Profile Configuration se nastaví hodnota Number of Rows na 1. Zobrazí se lišta, ve které se v řádku Enter Profile Name vyplní název wlan\_testing. V záložce Application se do hodnoty Rows napíše 1 a zobrazí se další lišta, kde se zvolí možnost File Transfer Heavy. Vše ostatní se ponechá beze změny a vybrané parametry se potvrdí tlačítkem Ok. V liště

(Profile Configuration) Table je vše již nastaveno a proto je už třeba pouze potvrdit tlačítkem Ok. Konfigurace se zavře tlačítkem Ok. Poté se označí všechny tři stanice a pravým kliknutím se vstoupí do jejich konfigurace. V záložce Application: Supported Profiles se nastaví hodnota Number of Rows na 1. Objeví se řádek, na kterém je napsáno Profile Name. Po rozkliknutí se nabízí možnost již předem vytvořeného profilu wlan\_testing. Vše se potvrdí Ok. V liště Attributes se zaškrtně možnost Apply to selected objects. Vše se poté potvrdí tlačítkem Ok. Pro konfiguraci serveru s názvem ethernet\_server se opět pravým tlačítkem klikne na vybranou komponentu a zvolí se možnost Edit Attributes. V záložce Application: Supported Services se hodnota Rows nastaví na 1. V záložce Name se zvolí možnost File Transfer Heavy. Vše se potvrdí tlačítkem Ok.

### **3) Nastavení a zobrazení statistik**

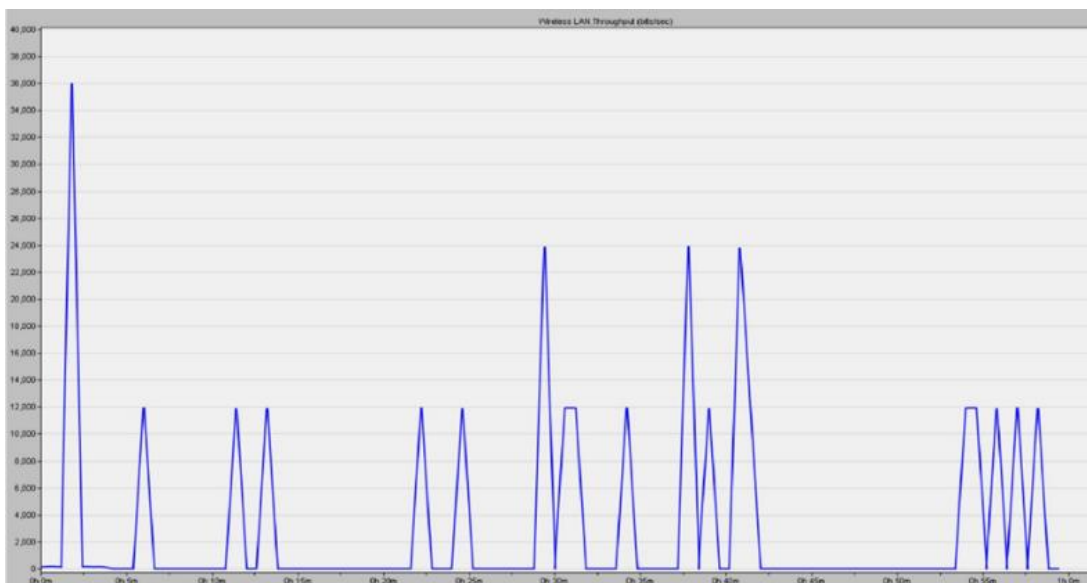
Pro nastavení vybraných statistik se pravým tlačítkem klikne na plochu na libovolné místo a v zobrazené liště se zvolí možnost Choose Individual DES Statistics. Zobrazí se lišta Choose Result, ve které se navolí statistiky, které se mají poté zobrazit. V záložce Global Statistics se vybere možnost Ethernet => Delay (sec). V záložce Global Statistics je nutné ještě označit Wireless LAN, kde se také označí Delay (sec). V horní liště se zvolí Run (běžící postava). Duration se nastaví na 1 hodinu (hours) a Values per statistics se nastaví na 100. Poté se stiskne tlačítko RUN. Objeví se lišta Simulation Progress: wlan\_testing – Scenario, kde je možné sledovat průběh simulace. Až simulace skončí, zobrazí se hlášení Simulation Completed. Vše se zavře a v horní záložce Result Browser se zobrazí výsledné grafy z měření. Ze záložky DES Graphs se zvolí Results for: Current Scenario. V záložce Global statistics se vybere možnost grafu pro Delay (sec). V záložce Presentation se zvolí možnost Stacked Statistics a time\_average pro přehlednost zobrazení výsledného grafu.

Pro nastavení statistiky Throughput (bits/sec) je nutné kliknout na plochu pravým tlačítkem a vybrat možnost Choose Individual DES Statistics. V liště Choose Result je nutné vybrat záložku Global Statistics => Wireless LAN => Throughput (bits/sec). Dále zvolit v liště Node Statistics => Wireless LAN => Throughput (bits/sec). Poté nastavení uložit a spustit simulaci nastavenou na 1 hodinu a Values per statistics na hodnotu 100. Po skončení simulace kliknout v horní liště na View Results a zobrazit lištu Results

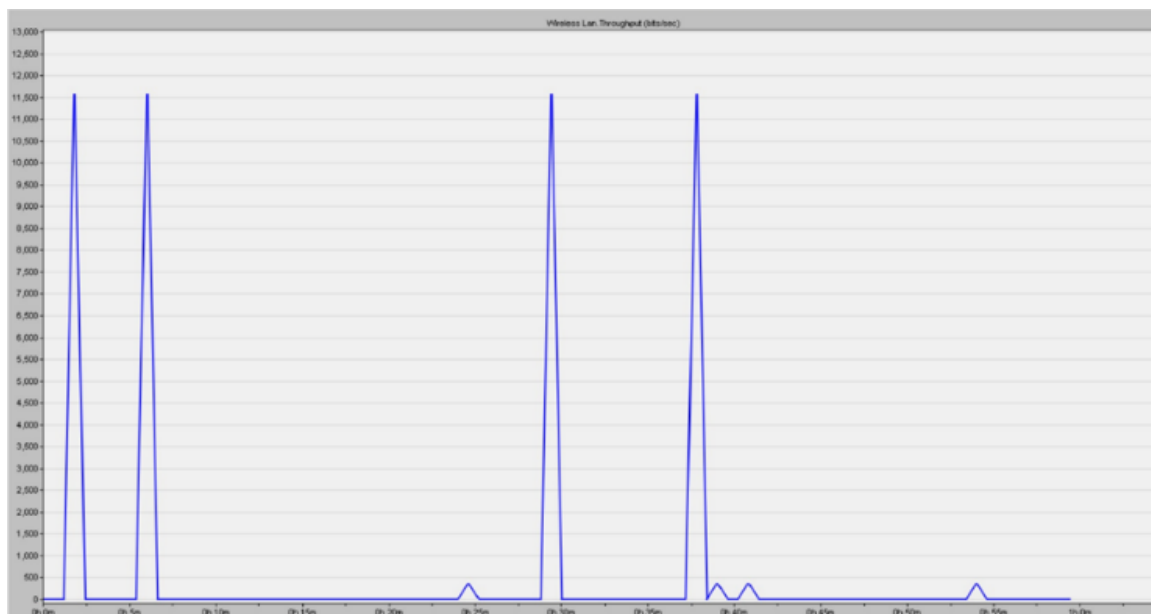
Browser. Zde vybrat možnost Current Scenario a již vytvořený project. Poté kliknout na Global Statistics => Wireless LAN => zatrhnout možnost Throughput (bits/sec). Tím se zobrazí graf zahazování Troughput (bits/sec). Pro přehlednost je lepší vždy zobrazovat pouze jednotlivé grafy. To lze docílit tlačítkem Show ve spodní části pravé strany obrazovky. Grafy je vhodné ukládat na flash disk, nebo pomocí printscreen. Nakonec zbývá zobrazit graf načítání jednotlivých routerů pro porovnání. Postup je stejný jako v předchozích případech jenom se v liště Global Statistics zvolí možnost Wireless LAN => Load (bits/sec). A v záložce Node Statistics se zatrhne možnost Wireless LAN => Load (bits/sec) a Queue Size (packets). V horní liště se zvolí možnost Run s nastavenými parametry 1 hodina a Values per statistics. Po skončení simulace zobrazit View Results v horní liště programu a zobrazit statistiky Node Statistics. Vybrat záložku Wireless LAN a zaškrtnout Load (bits/sec) a Queue Size (packets). Presentation zvolit jako Stacked Statistics a dále pak zvolit average.

#### 4) Zobrazení Grafů

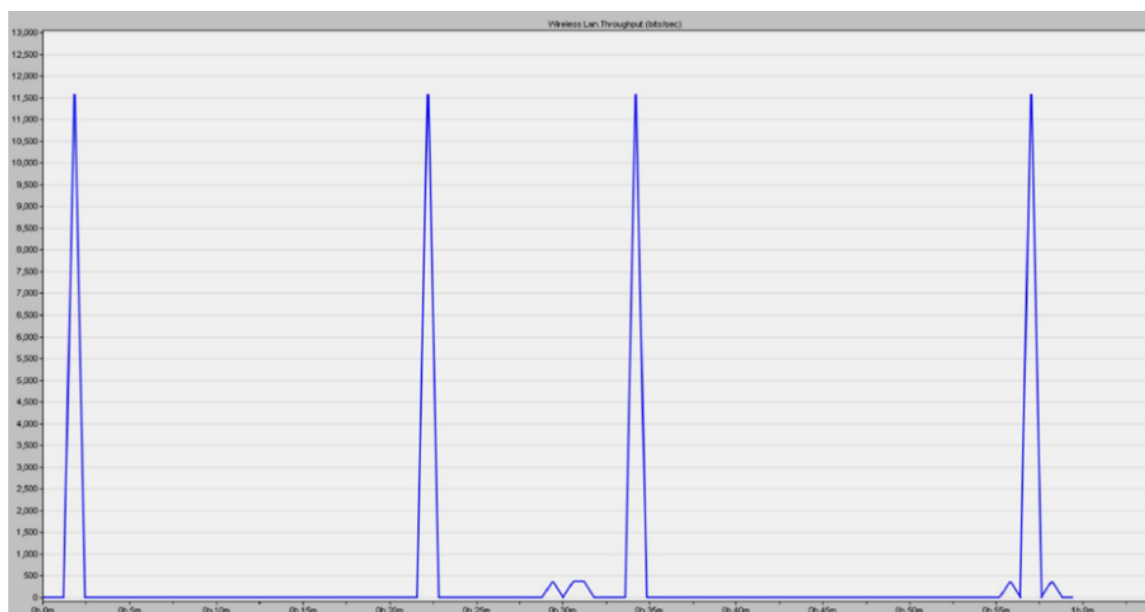
Jednotlivé grafy jsou zobrazeny níže:



Obr. 4: Celková propustnost jednotlivých routerů

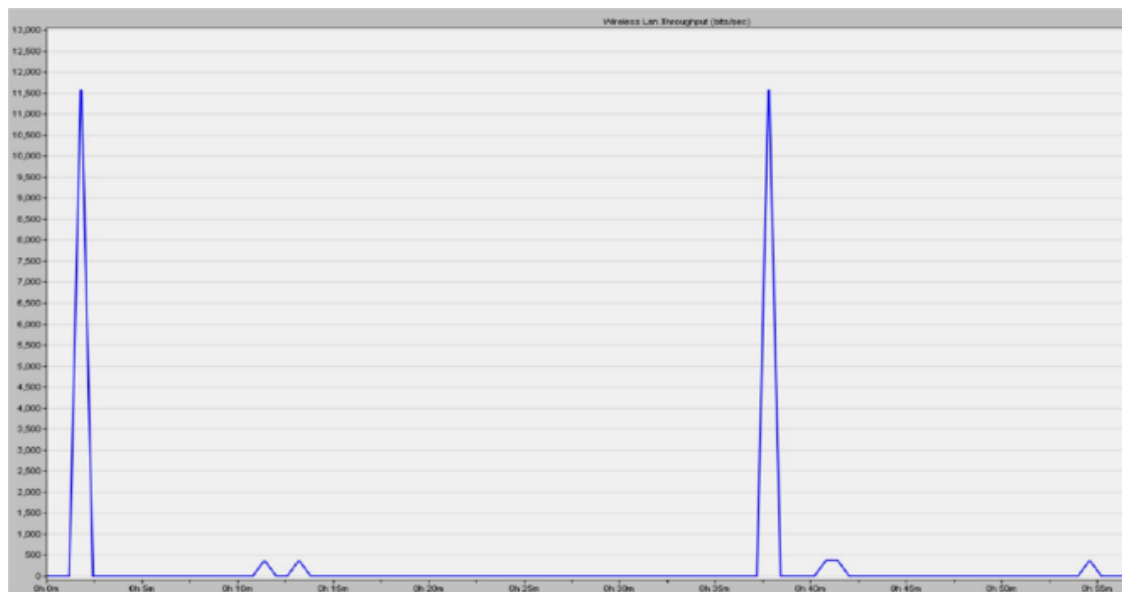


Obr. 5: Propustnost routeru 1

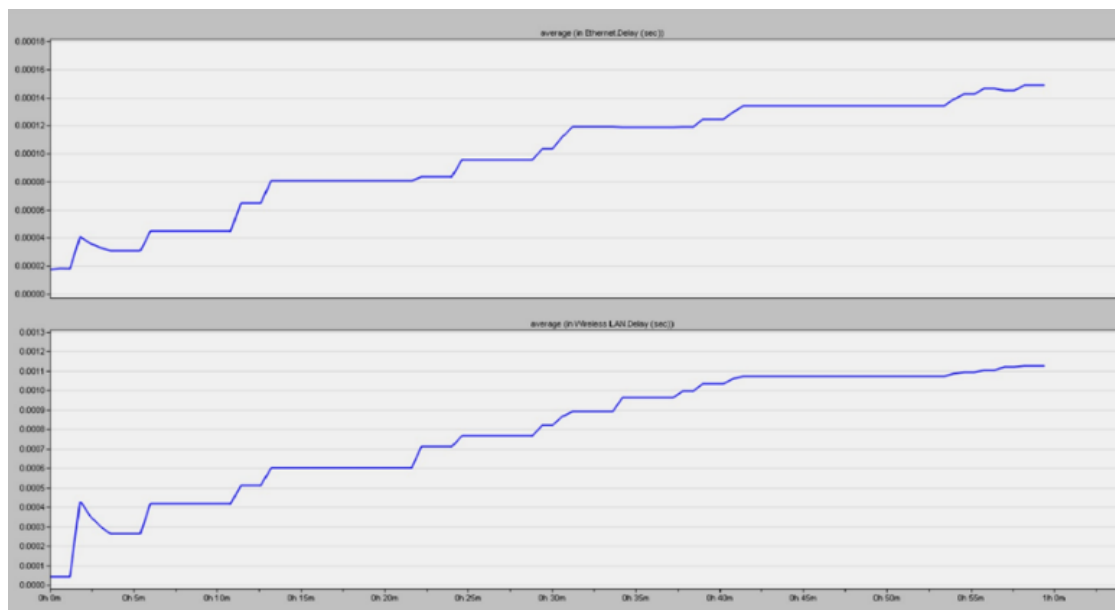


Obr. 6: Propustnost routeru 2





Obr. 7: Propustnost routeru 3



Obr. 8: Zpoždění

## **5) Popis grafů**

U grafu zpoždění je opatrné, že během časového úseku, který trval 1 hodinu, tak docházelo k postupnému nárustu zpoždění. Na x-ové ose je vidět čas simulace v programu Riverbed v minutách a na y-ové ose je zpoždění v sekundách. V čase 2,5 minuty došlo k nárustu zpoždění z nuly na více jak 4 sekundy. To je způsobeno tím, že bylo nastaveno File Transfer Heavy při konfiguraci Application Config a Profile Config. Standard 802.11g využívá pásmo 2,4 GHz a přenosovou rychlost 54 Mbit/s. Reálná přenosová rychlost během přenosu však byla mnohem menší. To způsobilo kolísání zpoždění, kdy v časech 2,5 minuty, 12 minut, 22 minut, 32 minut, 42 minut docházelo k výkyvům zpoždění. Zpoždění se ustálilo až po 42 minutách měření.

U grafu propustnosti routeru 1 je vidět, že je tento router podobně jako router 3 ovlivněn buď topologií sítě (odchýlení, vzdálenost) a nebo jeho nastavením (kanál), kdy nebylo možné nastavit jeden kanál ale tento kanál se vybíral náhodně. To mohlo způsobit ovlivnění propustnosti všech těchto routerů. Z grafu je také patrné, že tento router zachytával a propouštěl nejvíce dat ve 2 minutách, 6 minutách, 28 minutách a 38 minutách. Ke konci simulace tento router již nevykazoval téměř žádnou aktivitu

U grafu propustnosti routeru 2 je vidět, že měl tento router během hodinové simulace nejstabilnější propustnost. Tento router data aktualizoval nejenom na začátku simulace, ale i v průběhu a na konci simulace. To může být způsobeno jeho umístěním do pomyslné přímky v topologii sítě. Tyto výsledky mohly být také ovlivněny nastavením routeru, kdy v programu nešel přímo nastavit kanál, ale tento kanál se nastavoval automaticky pro každý router. I to mohlo způsobit kolísání a propustnost dat jen v určitý okamžik simulace.

U grafu propustnosti routeru 3 je vidět, že měl tento router během hodinové simulace největší okamžik propustnosti ve 2 minutách a ve 48 minutách. Z grafu je také patrné, že samotná propustnost dat u routeru 3 ukazuje mnohem více nulových dat než u routeru 1 a routeru 2. Tato nulová data mohou být způsobena topologií sítě (router 3 byl odchýlen, moc vzdálen), mohla být také způsobena nastavením routeru (kanál).

Z grafu celkové propustnosti je vidět, že byl ale přenos a propustnost dat v průběhu celé simulace. Což bohužel ale vypovídá tomu, že když chtěl data posílat jeden router, tak druhý ho neblokoval. Vypovídá to však také o tom, že celková propustnost v síti je zhruba poloviční, oproti propustnosti jednotlivých routerů, ale dostačující. Není zde vidět moc dat, které se vůbec nepřenesly.

## **6) Cíle první laboratorní úlohy**

Tato laboratorní úloha má poukázat na to, jak se vzájemně ovlivňují WLAN sítě, které jsou v dnešní době velmi rozšířené. V každé domácnosti se nachází tato technologie WLAN, ale mnoho lidí pořádně neví, jak přesně tato technologie funguje. Díky jednoduché instalaci však není možné správně pochopit, jak WLAN vlastně fungují. Je mnoho možností, jak zlepšit správné fungování WLAN tak, aby přenos po síti byl mnohem rychlejší a WLAN tak mnohem výkonnější. Vše záleží na správné volbě routeru, jehož parametry tento přenos ovlivňují. Volba standardu, který router podporuje, frekvenční pásmo, přenosovou rychlost, modulaci a zisk antén. Nejeefektivněji bude fungovat router se standardem 802.11ac, který nejenom, že podporuje frekvenční pásmo 5 GHz, které oproti pásmu 2,4 GHz není tak využívané, ale podporuje i mnohem větší přenosovou rychlost, která je pro přenos důležitá. Nicméně neposkytuje takový komunikační dosah jako standardy IEEE 802.11 v pásmu 2,4 GHz.

V laboratorní úloze je však nutné podotknout, že ovlivnění v pásmu 5GHz není možné dosáhnout bez nutného zahlcení sítě. Proto je v laboratorní úloze zvolen standard 802.11g, který podporuje pásmo 2,4 GHz a jeho zahlcení je tudíž možné i bez většího zahlcení sítě. Cílem laboratorní úlohy je poukázat na to, že ve frekvenčním pásmu 2,4 GHz dochází k jednoduššímu zahlcení přenosu i v program Riverbed, který není přesně určen na testování WLAN sítí. Student by měl být schopen pochopit rozdíl ve využívání přenosových rychlostí. Program Riverbed jich nabízí hned několik pro lepší porovnání. Program Riverbed je mnohem snadnější na konfiguraci jednotlivých parametrů oproti jiným programům a tak studenti mohou do značné míry zkoušet jednotlivá nastavení i pro standardy, které se v laboratorní úloze nevyužívají. Pochopení nastavení jednotlivých parametrů je obrovským přínosem v rámci pochopení této problematiky. V praxi se pak studenti mohou obeznámit s tím, že výběr vhodného routeru je opravdu důležitý, i když je jeho cena poněkud vyšší oproti dostupnějším levnějším routerům. Studenti se naučí zobrazit a pochopit význam parametrů Delay a Throughput. Dokážou vysvětlit jejich rozdíl a důležitost v rámci QoS.

### 4.3 Druhá laboratorní úloha – HW sestavení

Při měření první části se úloha zapojila v domácím prostředí dle následující topologie: RPi 3 (iperf3Server), RPi Zero (iperf3Client) a RPi 4 (iperf3Client/wifijammer). Zapojení úlohy je vidět na obázku níže:



Obr. 9: Zapojení laboratorní úlohy

K měření a ověření parametrů přenosu TCP a UDP byly použity routery Mercusys, Netis, TP-Link a Asus. Tyto routery byly postupně měněny a testovány na určení parametrů přenosu v čase 10 minut. Byl k tomu využit program Iperf3, který byl nainstalován na všech třech Raspberry Pi. V programu Iperf3 se uskutečnilo testování protokolů TCP a UDP. Oba tyto protokoly měly nastavené určité parametry během testování.

Během testování se postupně měnily a nastavovaly všechny čtyři routery.

Při přihlášení routerů bylo nutné zadat přihlašovací jméno a heslo, které bylo pro jednoduchost nastaveno u všech routerů stejně.

Přihlašovací jméno: student1234
Heslo: student1234

Jakmile byly zadány požadované přihlašovací údaje, v sekci Wireless, se v poli Mode, zvolil požadovaný standard (IEEE 802.11b only, IEEE 802.11n only), v poli Channel byl kanál nastaven na volbu automatic, v poli Channel Width byla zvolena šířka pásma dle možností požadovaného standardu. Standard IEEE 802.11 b podporuje šířku pásma pouze 20 MHz. Standard IEEE 802.11n má možnost zvolení šířky pásma 20 MHz a 40 MHz.

Důležitým posledním krokem bylo, aby bylo SSID nastaveno na RPi. Až tohle vše bylo zkontrolováno a vybráno, tak se vše potvrdilo ve spodní části okna tlačítkem save.

Parametr  $-b$  určuje maximální rychlost přenosu daného routeru. Tento parametr se tedy měnil s výměnou routeru a s jiným nastavením standardu na routeru.

Pro router Mercusys se standardem 802.11 b byl parametr  $b$  zvolen na  $-b$  20m

Pro router Mercusys se standardem 802.11 n byl parametr  $b$  zvolen na  $-b$  350m

Pro router Netis se standardem 802.11 b byl parametr  $b$  zvolen na  $-b$  20m

Pro router Netis se standardem 802.11 n byl parametr  $b$  zvolen na  $-b$  150m

Pro router Tp-Link se standardem 802.11 b byl parametr  $b$  zvolen na  $-b$  20m

Pro router Tp-Link se standardem 802.11 n byl parametr  $b$  zvolen na  $-b$  350m

Pro router Asus se standardem 802.11 b byl parametr  $b$  zvolen na  $-b$  20m

Pro router Asus se standardem 802.11 n byl parametr  $b$  zvolen na  $-b$  350m

Parametr  $-t$  určuje, jak dlouho probíhalo testování. Při testování routerů je tento parametr neměnitelný. Zůstává tedy na hodnotě  $-t$  600 (10 minut).

Parametr  $-u$  určuje, že se jedná o testování protokolu UDP, pro testování TCP není nutné nastavovat žádný parametr, neboť testování TCP je nastaveno defaultně.

Pro ukládání hodnot z měření do excelu je třeba využít příkaz:

```
>> D:\\název souboru.xls
```

Během testování ověření parametrů přenosu byly provedeny testy v čase 10 minut.

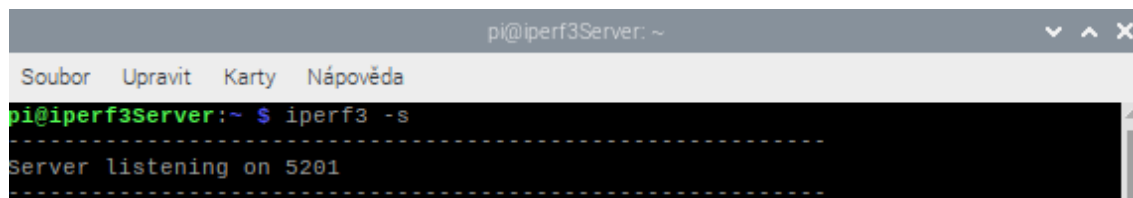
Během testování byly využity standardy IEEE 802.11 b a IEEE 802.11 n, na kterých byla nastavována šířka pásma, která se s použitím standardu měnila. U standardu IEEE 802.11 b byla použita šířka pásma 20 MHz. U standardu IEEE 802.11 n byly nastaveny šířky pásem na 20 MHz, 40 MHz a u routeru Asus i 80 MHz.

Kanál byl na routerech nastaven na volbu automatic. Výběr kanálu během testování bylo však možné zjistit pomocí příkazu:

```
iwlist wlan0 frequency
```

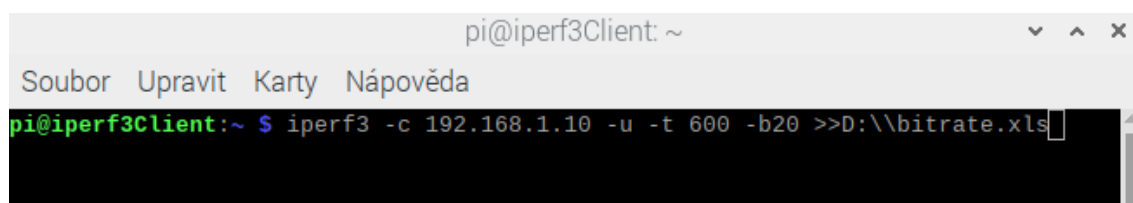
Zpracované tabulky jsou vloženy do příloh.

Celé nastavení parametrů s využitím programu Iperf3 je zobrazeno níže:



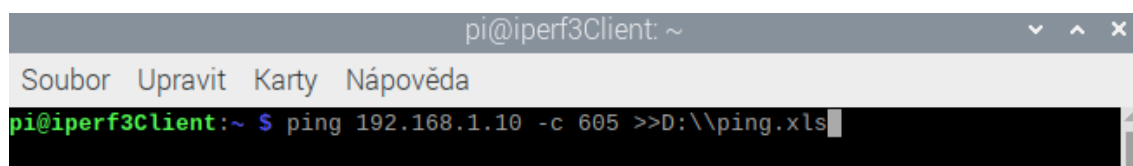
```
pi@iperf3Server: ~  
Soubor Upravit Karty Nápověda  
pi@iperf3Server:~ $ iperf3 -s  
-----  
Server listening on 5201  
-----
```

Obr. 10: Příkaz na RPi 3 (iperf3Server)



```
pi@iperf3Client: ~  
Soubor Upravit Karty Nápověda  
pi@iperf3Client:~ $ iperf3 -c 192.168.1.10 -u -t 600 -b20 >>D:\\bitrate.xls
```

Obr. 11: Příkaz na ověření propustnosti



```
pi@iperf3Client: ~  
Soubor Upravit Karty Nápověda  
pi@iperf3Client:~ $ ping 192.168.1.10 -c 605 >>D:\\ping.xls
```

Obr. 12: Příkaz na ověření zpoždění

RPi 3 (iperf3Server) byl připojen k monitoru, klávesnici a myši. Ale je možné využít vzdálený přístup ke všem třem Raspberry Pi. Tento přístup je možný pomocí VNC Viewer, ve kterém se nastaví IP adresa, name a heslo a je možné díky tomuto přístupu ovládat všechny Raspberry Pi bez použití klávesnic, monitorů a myši. V příkazovém řádku se pomocí příkazu

```
ifconfig
```

zjistila IP adresa serveru.

```
iperf3 -s
```

Druhým příkazem se zaručilo, že server bude naslouchat po dobu testování na portu 5201. Iperf 3 client byl také připojen k monitoru, klávesnici a myši. Nastavení parametrů bylo ve dvou příkazových řádcích.

V prvním příkazovém řádku na testování propustnosti bylo nastaveno:

```
iperf3 -c 192.168.x.x -u ( při testování TCP bylo políčko před parametrem -t volné) -t 600  
-b (20, 200 nebo 350 podle možností přenosových rychlostí routerů) >> D:\\název  
souboru.xls
```

Paralelně k tomuto řádku byl otevřen druhý příkazový řádek na testování zpoždění s příkazem:

```
ping 192.168.x.x -c 605 >> D:\\název souboru.xls
```

Parametr *-c* značí, jak dlouho bude zpoždění testováno.

Ověření parametrů přenosu bylo testováno jak pro RPi Zero, tak pro RPi 4. Měnilo se tak pouze zapojení klienta v dané topologii. Vše ostatní zůstalo beze změn.

Po spuštění se vyčkalo 10 minut uložení hodnot do dvou souborů. Jakmile testování skončilo, v již otevřené aplikaci Bitvise bylo zadáno:

*Host: IP dresa RPi Zero (iperf3Client)*

*Port: 22*

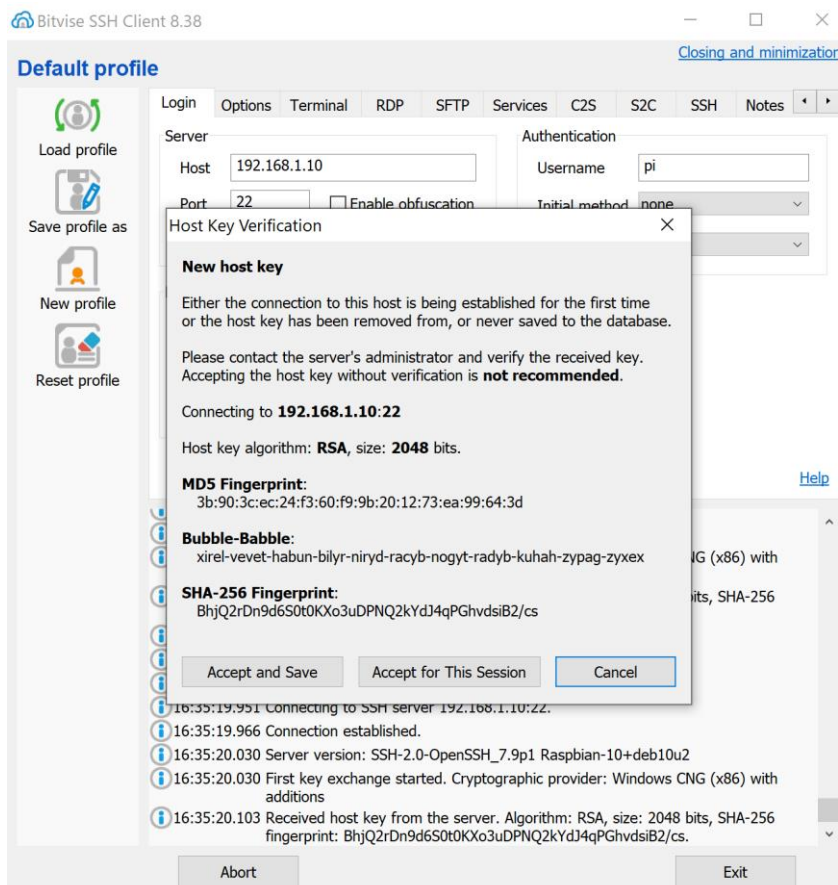
*Username: pi*

dále se kliknulo na Log in. Poté se zaškrtnulo Accept for This Session a objevilo se okno, kde se zadá heslo

heslo: raspberry

Poté byl postup stejný jako při používání Total Commander.





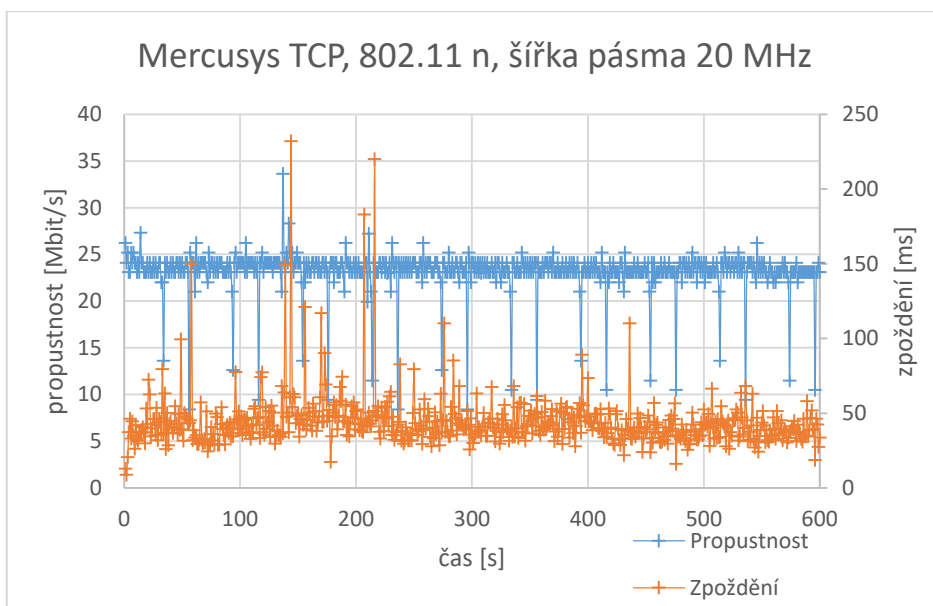
Obr. 13: Postup při zpracování dat v aplikaci Bitvise

Z naměřených hodnot byly poté zpracovány grafy. Jelikož samotné testování na deset minut pro TCP a UDP protokoly naměřilo a uložilo 1200 hodnot jen pro standard 802.11 b pro šířku pásma 20 MHz, bylo nutné ostatní hodnoty a grafy uložit do příloh a zde zobrazit a popsat pouze ty, u kterých byly naměřené hodnoty nejzajímavější.

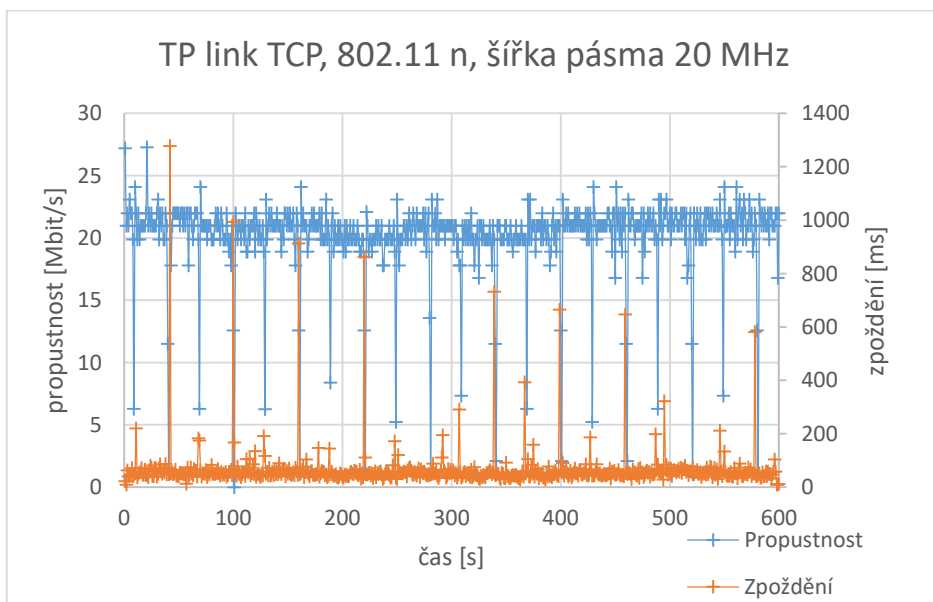
Proto jsou zde vybrány grafy pro router s nejlepšími hodnotami během přenosu a pro router, který měl během přenosu výsledné hodnoty nejhorší.

Při testování ověřování parametrů přenosu s použitím Raspberry Pi Zero na tom byl z hlediska přenosových rychlostí nejlépe router Mercusys, který měl nejvyšší přenosové rychlosti při použití standardu IEEE 802.11 n. Přenosovou rychlost pro standard IEEE 802.11 b s šířkou pásma 20 MHz měl však router Mercusys nejhorší, neboť se pohybovala pouze v řádech Kbit/s. Pro standard IEEE 802.11 n měl router Mercusys přenosovou rychlost 23,1 Mbit/s s použitou šířkou pásma 20 MHz. Nejhuře při testování ověření parametrů přenosu dopadly routery Asus a TP-Link. Při testování zpoždění vykazoval nejmenší zpoždění při přenosu router Asus a naopak nejhuře dopadly routery Netis a

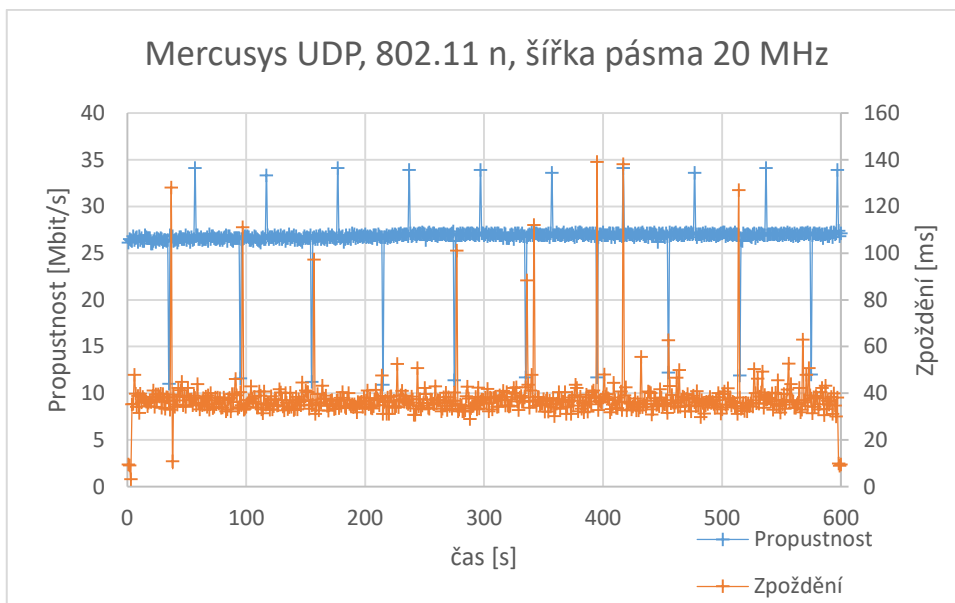
TP- Link, které vykazovaly během přenosu nejvyšší hodnoty pro zpoždění. Router Asus měl nejmenší zpoždění 662 ms při přenosu UDP s použitou šířkou pásma 40 MHz. Router Netis vykazoval zpoždění 1549 ms při přenosu UDP s použitou šířkou pásma 20 MHz. Hodnota zpoždění pro router TP-Link byla 1524 ms při přenosu UDP s použitou šířkou pásma 20 MHz s využitím standardu IEEE 802.11 b.



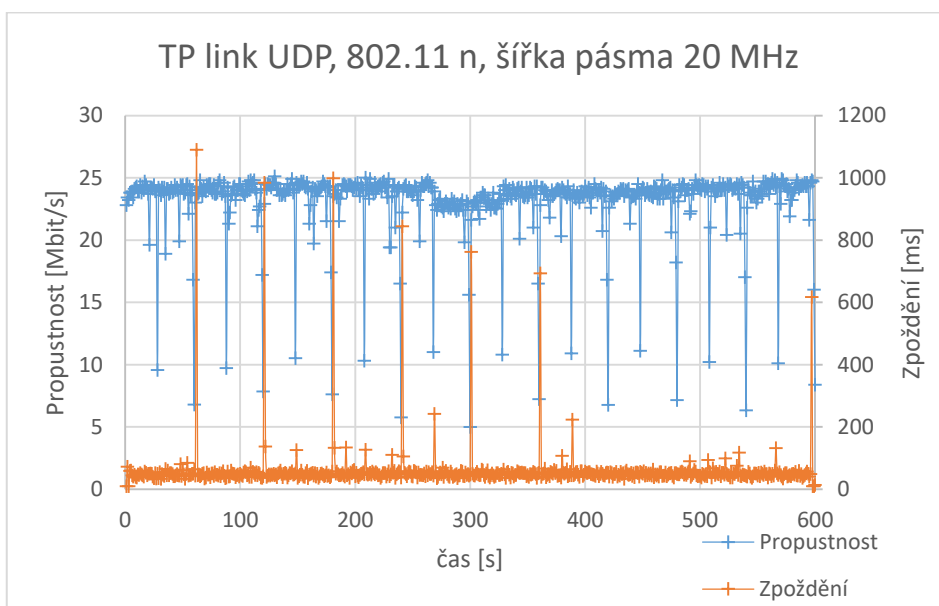
Obr. 14: Přenos TCP pro router Mercusys s použitým standardem 802.11 n.



Obr. 15: Přenos TCP pro router TP-Link s použitým standardem 802.11 n.



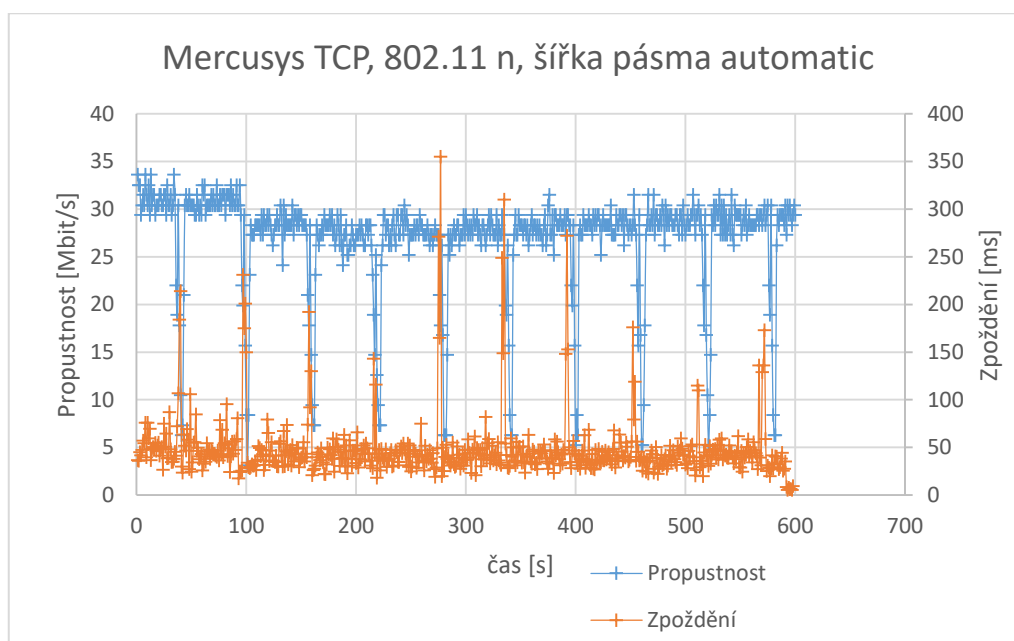
Obr. 16: Přenos UDP pro router Mercusys s použitým standardem 802.11 n.



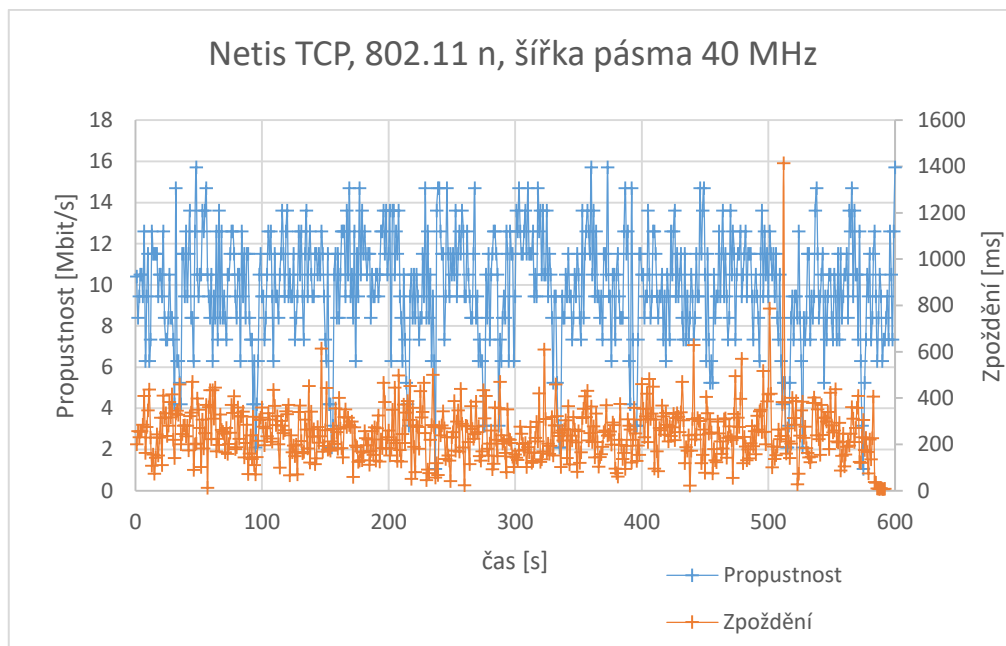
Obr. 17: Přenos UDP pro router TP-Link s použitým standardem 802.11 n.

Při testování ověření parametrů přenosu s použitím RPi 4 měl nejvyšší přenosovou rychlost router Mercusys a naopak nejmenší přenosovou rychlost měl během testování router Netis. Pro zhodnocení přenosové rychlosti a zpoždění byl použit standard IEEE 802.11 n s řízkou pásma 40 MHz a s automatickou volbou šířky pásma pro srovnání. Pro router Mercusys byla přenosová rychlost 27,0 Mbit/s s použitou šířkou pásma automatic.

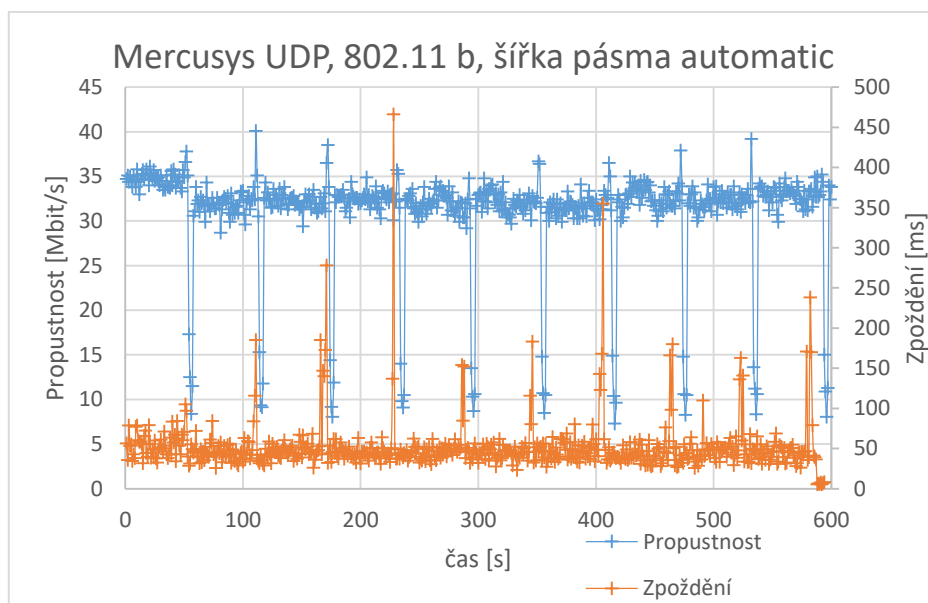
Pro router Netis byla přenosová rychlost pouhých 9,83 Mbit/s s použitou šířkou pásma 40 MHz. Při zpoždění dopadly nejlépe všechny routery kromě routeru TP-Link, který v testování vykazoval nejvyšší zpoždění. Toto zpoždění u routeru TP-Link bylo 1469 ms s použitou šířkou pásma 40 MHz. Zpoždění se u zbylých routerů pohybovalo 691 ms pro router Mercusys, 781 ms pro router Netis a 1408 ms pro router Asus. Celé toto testování probíhalo v pásmu 2,4 GHz. Jelikož router Asus jako jediný umožňuje přepnutí na pásmo 5 GHz, tak byly ověřeny parametry přenosu i na tomto pásmu. Router Asus při standardu 802.11 n s šířkou pásma 80 MHz dosahoval přenosové rychlosti až 60 Mb/s. Z tohoto důvodu bylo zvoleno RPi 4 pro ověření parametrů přenosu. RPi 4 dokáže totiž zachytávat přenos ve frekvenčním pásmu 5 GHz.



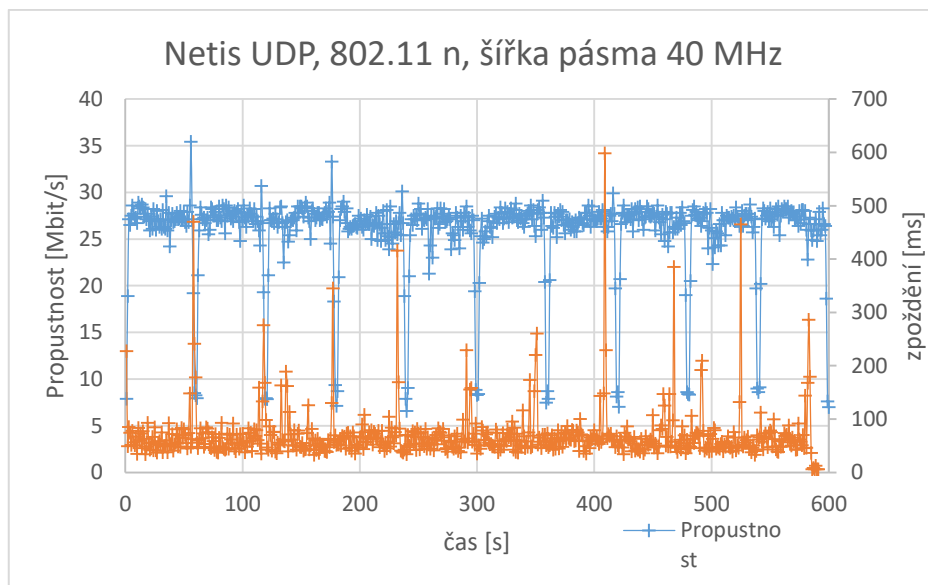
Obr. 18: Přenos TCP pro router Mercusys s použitým standardem 802.11 n.



Obr. 19: Přenos TCP pro router Netis s použitým standardem 802.11 n.



Obr. 20: Přenos UDP pro router Mercusys s použitým standardem 802.11 n.



Obr. 21: Přenos UDP pro router Netis s použitým standardem 802.11 n.

V druhé části úlohy se k RPi 3 (iperf3Server) a RPi Zero (iperf3Client) přidal RPi 4 v roli (iperf3Client/wifijammer). Ten měl pomocí skriptu wifijammer zahltit přenos v síti. Na RPi 4 (iperf3Client/wifijammer) bylo nejdříve nutné nainstalovat program scapy, python a poté wifijammer. Při spuštění programů bylo nejprve nutné zjistit, zda se parametry přenosu s využitím jednotlivých programů měnily.

Program scapy umožňoval několik druhů útoku na síť. Byly to zejména malformed packet, ping of death, nestea attack a land attack.

Během testování jednotlivých útoků na síť program nedokázal snížit přenosovou rychlost, zvýšit zpoždění, snížit propustnost a zvýšit ztrátovost.

Skript wifijammer, který je psaný v jazyce Python a využívá i program Scapy, už tyto hodnoty změnit dokázal. Pro správnou funkci skriptu je nutné mít nainstalován python 2.7, python-scapy a mít na zařízení připojenou externí WiFi kartu. Při ověření funkčnosti jednotlivých parametrů byl tento skript schopný na nějakou dobu deautorizovat síť v okolí. Po zvolení vhodných parametrů byl skript wifijammer schopný zahltit síť s využitím standardů IEEE 802.11 b a IEEE 802.11 n.

RPi 4 (iperf3Client/wifijammer) byl ovládán pomocí vzdáleného přístupu. Během testování bylo kontrolováno, zda je zařízení připojeno k síti RPi a zda je stabilní připojení. V příkazovém řádku byl zadán příkaz,

```
ls
```

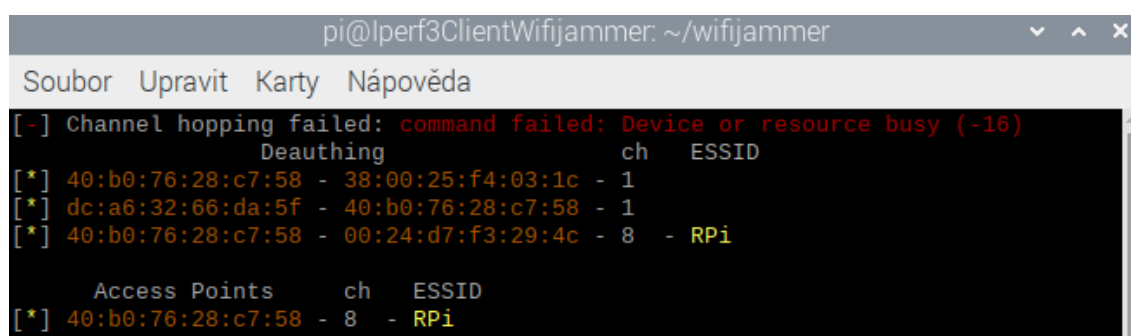
který ukázal, zda je ve složce soubor wifijammer.py. Po přepnutí do složky, která obsahuje soubor wifijammer.py, se bylo možné dostat pomocí příkazu

```
cd wifijammer/
```

Aby bylo možné program ovládat, je nutné být v režimu superuživatele. To bylo provedeno příkazem

```
sudo python wifijammer.py
```

Pak se tento příkaz potvrdil tlačítkem enter. Po zadání a potvrzení příkazu se program spustil ale zároveň deautorizoval všechny sítě v okolí. Také však zobrazil použitou MAC adresu RPi, kterou bylo nutné si zaznamenat. Viz obrázek níže:



```
pi@lperf3ClientWifijammer: ~/wifijammer
Soubor Upravit Karty Nápověda
[-] Channel hopping failed: command failed: Device or resource busy (-16)
      Deauthing      ch  ESSID
[*] 40:b0:76:28:c7:58 - 38:00:25:f4:03:1c - 1
[*] dc:a6:32:66:da:5f - 40:b0:76:28:c7:58 - 1
[*] 40:b0:76:28:c7:58 - 00:24:d7:f3:29:4c - 8 - RPi

      Access Points      ch  ESSID
[*] 40:b0:76:28:c7:58 - 8 - RPi
```

Obr. 22: Zobrazení MAC adresy zařízení RPi.

Poté už jen stačilo sestavit testovací parametry pro program wifijammer. Celý příkaz na testování:

```
sudo python wifijammer.py -a x:x:x:x:x:x -c x -d -i wlan0 -p x -t x
```

kde:

-a značí použitou MAC adresu RPi

-c označuje kanál, na kterém dané RPi vysílá. Tento kanál byl pro všechna RPi zvolen stejně. A bylo možné jej zjistit vedle zobrazené MAC adresy.

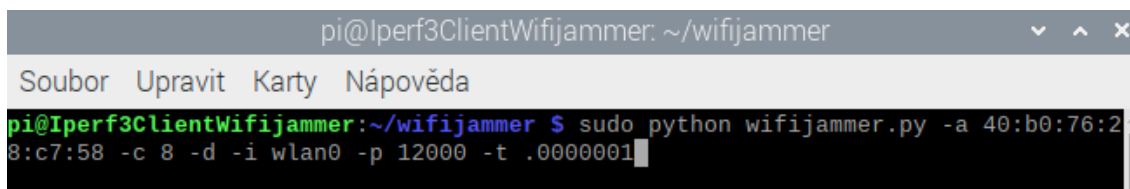
-d značí, že se nebude deautorizovat síť v průběhu vysílání

-i značí použité rozhraní

-p označuje počet paketů, které byly během testování odeslány. Pro standard 802.11 b byla hodnota odeslaných paketů nastavena na 1200. Při větší hodnotě docházelo k výpadku celé komunikace. Pro standard 802.11 n byla tato hodnota nastavena na 25000. Při větší hodnotě už opět docházelo k výpadkům komunikace.

-t označuje čas, za který se tyto pakety opakovaně přenášely. Pro testování byla zvolena hodnota 0.00000001 s.

Blíže je tento příkaz vidět na obrázku níže.



```
pi@lperf3ClientWifijammer: ~/wifijammer
Soubor Upravit Karty Nápověda
pi@lperf3ClientWifijammer:~/wifijammer $ sudo python wifijammer.py -a 40:b0:76:28:c7:58 -c 8 -d -i wlan0 -p 12000 -t .00000001
```

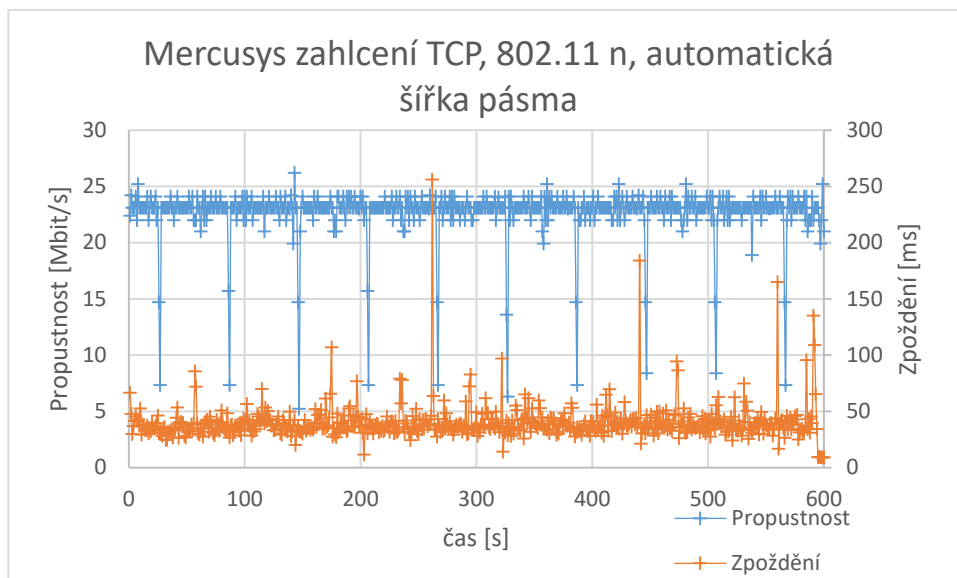
Obr. 23: Příkaz pro zahlcení standardu 802.11 b

Během testování jaminngu bylo nutné nejprve spustit příkazem server, poté program wifijammer a nakonec klienta, na kterém byly paralelně nastaveny příkazy na testování propustnosti a zpoždění při přenosu.

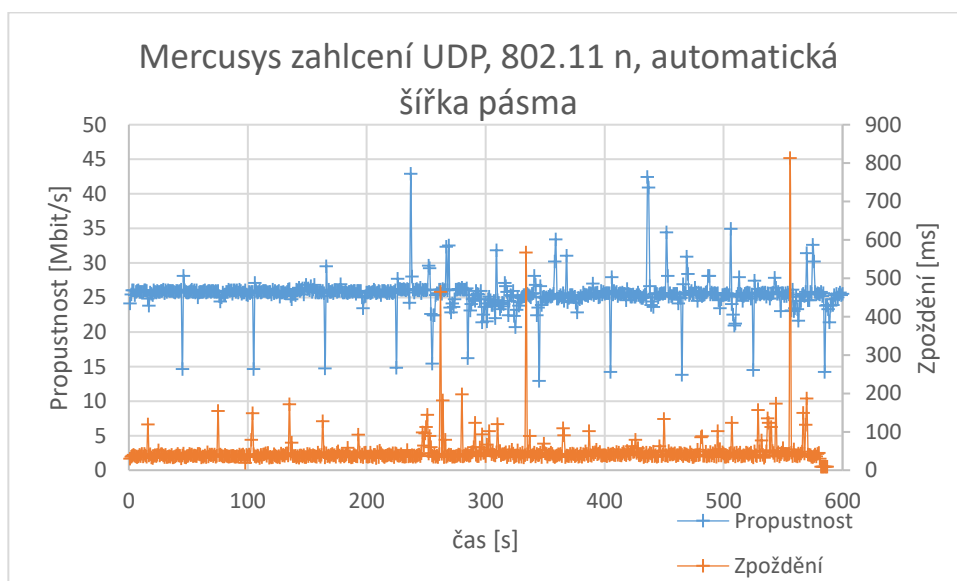
Po testování, které trvalo 10 minut, bylo nutné uložené hodnoty zpracovat do přehledných grafů.

Nejmenší zpoždění vykazoval router Asus při standardu 802.11 n s šířkou pásma 40 MHz. Při přenosu TCP u routeru Asus byla hodnota zpoždění 1129 ms. Při použití standardu IEEE 802.11 b měl však nejmenší zpoždění při zatížení router Mercusys. Při přenosu UDP byla tato hodnota 894 ms. Při zatížení a testování standardu IEEE 802.11 n vykazoval nejhorší výsledky router Mercusys, kterému se nejenom snížila přenosová rychlost, propustnost, ale i zvýšilo se zpoždění a ztráta paketů. Při zatížení se hodnota přenosové rychlosti snížila na 24,2 Mbit/s z původních 30,7 Mbit/s při přenosu UDP. Zatímco hodnota zpoždění byla před zatížením 748 ms při přenosu UDP, tak po zatížení tato hodnota narostla na 966 ms. Před zatížením vykazoval router Mercusys ztrátovost 1,4 % s využitím standardu IEEE 802.11 n s automatickou volbou šířky pásma. Po zatížení se tyto ztráty zvýšily na 4,8 %.

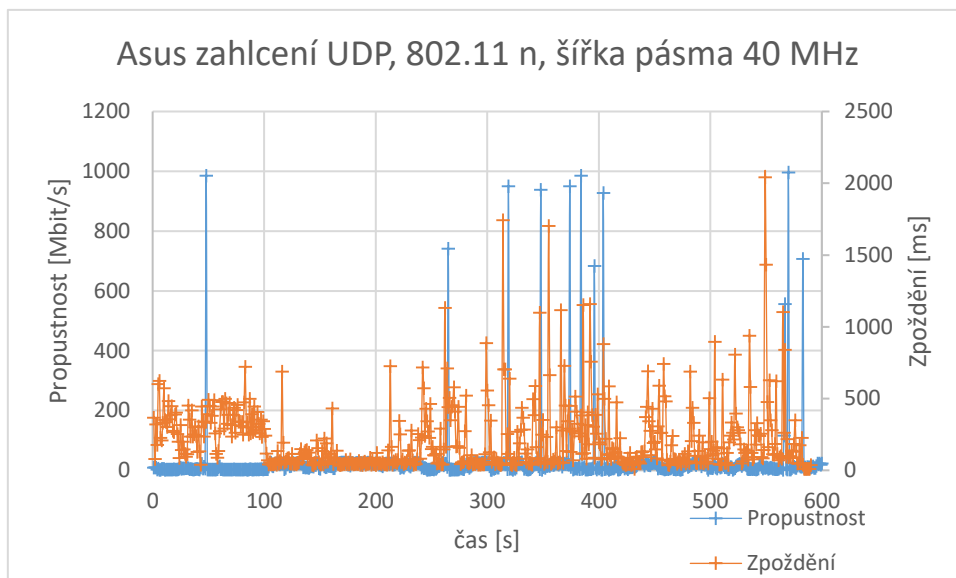




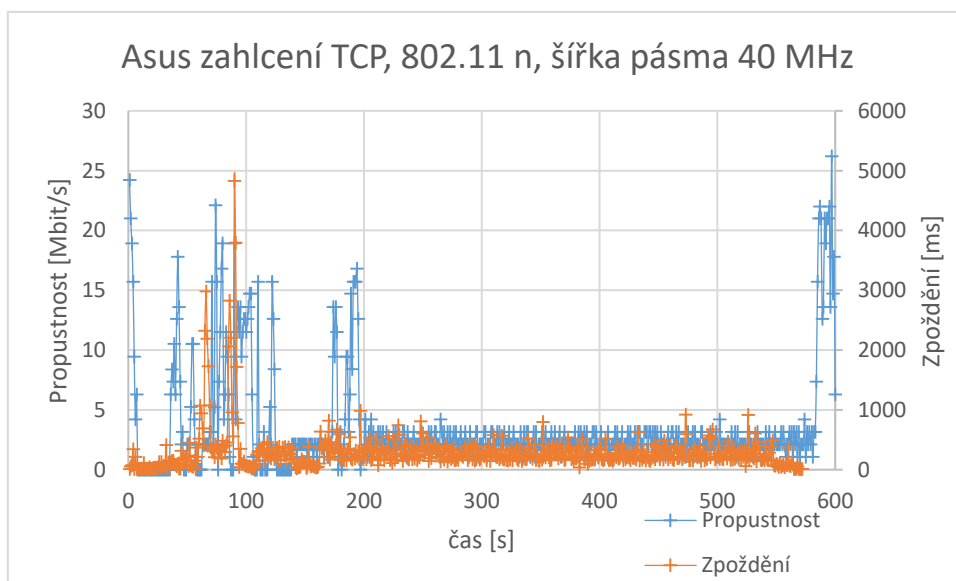
Obr. 24: Přenos TCP pro router Mercusys s použitým standardem 802.11 n.



Obr. 25: Přenos UDP pro router Mercusys s použitým standardem 802.11 n.



Obr. 26: Přenos UDP pro router Asus s použitým standardem 802.11 n.



Obr. 27: Přenos TCP pro router Asus s použitým standardem 802.11 n.

### **Cíle druhé laboratorní úlohy**

Druhá laboratorní úloha má poukázat na to, jak se vzájemně ovlivňují a ruší WLAN sítě. Zahlcení sítě a zhoršení komunikačních parametrů bylo docíleno pomocí skriptu wifijammer, který byl nainstalován na Raspberry Pi 4. V laboratorní úloze byly testovány postupně čtyři routery (Mercusys, Netis, TP-Link a Asus s vybranými standardy IEEE 802.11. Aby bylo možné, co největšího zahlcení sítě, byl zvolen standard IEEE 802.11 b s přenosovou rychlostí 11 Mbit/s. Jelikož tento standard vysílá v pásmu 2,4 GHz, byl z hlediska náchylnosti na rušení tou nejlepší volbou. Druhý byl zvolen standard IEEE 802.11 n, jehož přenosová rychlost dosahuje až 300 Mbit/s. Nutného zahlcení mohlo dojít reálným způsobem jako je stahování torrentů, sledování videí, hraní her, atd. Druhou možností bylo zahlcení pomocí vhodného skriptu, který umožnil stahování několik tisíc paketů za piko sekundu. Program Scapy umožnil síť atakovat pomocí vhodných útoků, avšak ani jeden z těchto útoků neovlivnil a nezahltit síť dostatečně. Byly to zejména útoky Malformed packets, ping of death, nestea attack a land attack. Skript wifijammer, který nabízí několik možností atakování sítě je k tomuto zahlcení a rušení nejideálnější. Dokázal deautorizovat síť, zahltit ji a nebo také úplně odpojit. Cílem této laboratorní úlohy bylo ověřit parametry přenosu v síti pomocí protokolů TCP, UDP a následně zahltit tuto síť pomocí wifijammer. Student by měl být, stejně jako v první laboratorní úloze, schopen pochopit rozdíl ve využívání přenosových rychlostí, standardů a šířek pásem. Pochopení nastavení jednotlivých Raspberry Pi a jejich ovládání je obrovským přínosem v rámci pochopení této problematiky. Pomocí Raspberry Pi lze ovládat osvětlení, dveře, televizory a mnoho dalších zařízení. Důležité také je, aby studenti pochopili jaký je rozdíl mezi propustností, zpožděním a ztrátou paketů a jak se jejich ovlivnění zobrazí v grafech a v přenosu.

## 5 ZÁVĚR

První laboratorní úloha byla realizována v programu Riverbed Modeler. V předpokládaném závěru mělo nastat ovlivnění WLAN sítě pomocí zvolení vhodného standardu IEEE 802.11g s maximální teoretickou přenosovou rychlostí 54 Mbit/s, kmitočtovém pásmu 2,4 GHz a s nastavením kanálu číslo 6 pro všechny routery. V předpokládané hypotéze měla síť složená ze tří WiFi routerů prokazovat známky ztrátovosti a zpoždění při přenosu. V pásmu 2,4 GHz naslouchají jiná bezdrátová zařízení, která svým provozem toto kmitočtové pásmo značně zahltí. Ovlivňovat síť také může zvolená přenosová rychlost, která je pro přenos a kvalitu důležitým parametrem. Značného ovlivnění mělo být také docíleno zvolením vhodného kanálu, na kterém budou všechna tato zařízení naslouchat. V laboratorní úloze bylo možné docílit pouze zpoždění při přenosu a propustnosti. Výběr kanálu v programu Riverbed byl sice možný, ale během samotného testování zpoždění a propustnosti musel být nastaven defaultně pro zobrazení výsledných statistik. Program Riverbed je daleko vhodnější na testování FTP přenosu, Streamingu a dalších parametrů pro testování sítí. Avšak není moc vhodný na testování WLAN sítí, kde je nutná složitější konfigurace a potřebné zahlcení pro získání potřebných výsledků.

Druhá laboratorní úloha má poukázat na to, jak se vzájemně ovlivňují a ruší WLAN sítě. Rušení bylo docíleno pomocí skriptu wifijammer, který byl nainstalován na Raspberry Pi 4. V laboratorní úloze byly testovány postupně čtyři routery (Mercusys, Netis, TP-Link a Asus s vybranými standardy IEEE 802.11. Aby bylo možné, co největší rušení byl zvolen standard IEEE 802.11 b s přenosovou rychlostí 11 Mbit/s. Jelikož tento standard vysílá v pásmu 2,4 GHz, byl z hlediska náchylnosti na rušení tou nejlepší volbou. Druhý byl zvolen standard IEEE 802.11 n, jehož přenosová rychlost dosahuje až 300 Mbit/s. Zahlčení bylo docíleno pomocí vhodného programu, který umožnil stahování několik tisíc paketů za piko sekundu. Program Scapy umožnil síť atakovat pomocí vhodných útoků, avšak ani jeden z těchto útoků neovlivnil a nezahltit síť dostatečně. Skript wifijammer, který nabízí několik možností atakování sítě je k tomuto zahlcení a rušení nejideálnější. Dokázal deautorizovat síť a zahltit ji. Cílem této laboratorní úlohy bylo ověřit parametry přenosu v síti pomocí protokolů TCP, UDP a následně zahltit tuto

sít' pomocí wifijammer. Při testování ověřování parametrů přenosu s použitím Raspberry Pi Zero na tom byl z hlediska přenosových rychlostí nejlépe router Mercusys, který měl nejvyšší přenosové rychlosti při použití standardu IEEE 802.11 n. Přenosovou rychlost pro standard IEEE 802.11 b s šířkou pásma 20 MHz měl však router Mercusys nejhorší, neboť se pohybovala pouze v řádech Kbit/s. Pro standard IEEE 802.11 n měl router Mercusys přenosovou rychlost 23,1 Mbit/s s použitou šířkou pásma 20 MHz. Nejhorší při testování ověření parametrů přenosu dopadly routery Asus a TP-Link. Při testování zpoždění vykazoval nejmenší zpoždění při přenosu router Asus a naopak nejhorší dopadly routery Netis a TP-Link, které vykazovaly během přenosu nejvyšší hodnoty pro zpoždění. Router Asus měl nejmenší zpoždění 662 ms při přenosu UDP s použitou šířkou pásma 40 MHz. Router Netis vykazoval zpoždění 1549 ms při přenosu UDP s použitou šířkou pásma 20 MHz. Hodnota zpoždění pro router TP-Link byla 1524 ms při přenosu UDP s použitou šířkou pásma 20 MHz s využitím standardu IEEE 802.11 b. Při testování ověření parametrů přenosu s použitím RPi 4 měl nejvyšší přenosovou rychlost router Mercusys a naopak nejmenší přenosovou rychlost měl během testování router Netis. Pro zhodnocení přenosové rychlosti a zpoždění byl použit standard IEEE 802.11 n s šířkou pásma 40 MHz a s automatickou volbou šířky pásma pro srovnání. Pro router Mercusys byla přenosová rychlost 27,0 Mbit/s s použitou šířkou pásma automatic. Pro router Netis byla přenosová rychlost pouhých 9,83 Mbit/s s použitou šířkou pásma 40 MHz. Při zpoždění dopadly nejlépe všechny routery kromě routeru TP-Link, který v testování vykazoval nejvyšší zpoždění. Toto zpoždění u routeru TP-Link bylo 1469 ms s použitou šířkou pásma 40 MHz. Zpoždění se u zbylých routerů pohybovalo 691 ms pro router Mercusys, 781 ms pro router Netis a 1408 ms pro router Asus. Celé toto testování probíhalo v pásmu 2,4 GHz. Jelikož router Asus jako jediný umožňuje přepnutí na pásmo 5 GHz, tak byly ověřeny parametry přenosu i na tomto pásmu. Router Asus při standardu 802.11 n s šířkou pásma 80 MHz dosahoval přenosové rychlosti až 60 Mbits/s. Nejmenší zpoždění vykazoval router Asus při standardu 802.11 n s šířkou pásma 40 MHz. Při přenosu TCP u routeru Asus byla hodnota zpoždění 1129 ms. Při použití standardu IEEE 802.11 b měl však nejmenší zpoždění při zatížení router Mercusys. Při přenosu UDP byla tato hodnota 894 ms. Při zatížení a testování standardu IEEE 802.11 n vykazoval nejhorší výsledky router Mercusys, kterému se nejenom snížila přenosová rychlost, propustnost, ale zvýšilo se i zpoždění a ztráta paketů. Při zatížení se hodnota přenosové rychlosti

snížila na 24,2 Mbit/s z původních 30,7 Mbit/s při přenosu UDP. Zatímco hodnota zpoždění byla před zatížením 748 ms při přenosu UDP, tak po zatížení tato hodnota narostla na 966 ms. Před zatížením vykazoval router Mercusys ztrátovost 1,4 % s využitím standardu IEEE 802.11 n s automatickou volbou šířky pásma. Po zatížení se tyto ztráty zvýšily na 4,8 %. Toho bylo docíleno skriptem wifijammer, který tento router zahltil přenosem 1200 paketů za 0.0000001 s pro standard 802.11 b a pro standard 802.11 n zahltil tento přenos 25 000 pakety za 0.0000001 s. Bohužel u routerů Netis a TP-Link nedošlo ke snížení přenosové rychlosti a zvýšení zpoždění při využití skriptu wifijammer. Došlo pouze k větším ztrátám paketů. Ke snížení přenosové rychlosti a zvýšení zpoždění, ale došlo při měření parametrů u routeru Asus. U něj byla přenosová rychlost snížena o více jak polovinu. A to i při porovnání s pásmem 2,4 GHz. Co se ceny týče, tak router Mercusys lze na trhu sehnat okolo 300 Kč a router Asus za 1800 Kč. Proto je zajímavé jak si router Asus se zahlcením špatně poradil, ale routery Netis a TP-Link zvládly zahlcení výborně a dokonce oproti předchozímu testování na ověření parametrů přenosu, se jim zvýšila přenosová rychlost. Z hlediska konfigurace je však nejjednodušší router Mercusys, který má přehledně zpracované nastavení, zatímco nejnáročnější nastavení má router Asus, který má možnost vysílání jak na 2,4 GHz, tak na 5 GHz. Routery TP-Link a Netis by bylo také možné zahltit, avšak reálným provozem a nikoliv s využitím skriptu. Raspberry Pi i s využitím skriptu na zahlcení sítě nedokáže ovlivnit přenos v síti tak, aby došlo ke snížení přenosových rychlostí, zvýšení zpoždění a ovlivnění dalších parametrů. Reálným provozem je myšleno například stahování torrentů, streamování nebo hraní online her. V grafických přílohách jsou zobrazeny grafy pro měření s RPi Zero, RPi 4 a při zahlcení sítě. Pro velké množství dat jsou grafy zjednodušeny v podobě porovnání routeru, který z testování vyšel nejlépe a který naopak nejhůře. Jelikož byla laboratorní úloha zpracována v domácím prostředí nikoli v laboratorním, je možné, že se hodnoty naměřené studenty budou lišit. V okolí, kde byla tato laboratorní úloha realizována, bylo zachytáváno vysílání více než šesti WiFi routerů. Roli také mohla hrát vzdálenost jednotlivých zařízení od sebe. V domácím prostředí byla vzdálenost AP od Raspberry Pi přibližně metr. Toto měření je zaměřeno pouze na standardy IEEE 802.11 b a IEEE 802.11 n. Router Asus je ale primárně určen pro standard IEEE 802.11 ac a vysílání jak na pásmu 2,4 tak 5 GHz. V měření jsme ale tento standard nevyužili a až na jedno měření s RPi4 bylo 5 GHz pásmo vypnuté a standard byl nastaven

na IEEE 802.11 n. Toto nastavení tak mohlo ovlivnit chování routeru a proto nedosahoval vyšších přenosových rychlostí a menšího zpoždění než jaké bylo naměřeno.

# Literatura

- [1] Jeřábek, J. Komunikační technologie. Brno: Vysoké učení technické v Brně, 2019. s. 1-175. ISBN: 978-80-214-4713-4. (cs)
- [2] Molnár, K. Praktikum z informačních sítí. Brno: Vysoké učení technické v Brně, 2013. s. 1-135. ISBN: 978-80-214-4715-8. (cs)
- [3] Pužmanová, R. Moderní komunikační sítě A-Z. Computer Press, Brno 2007
- [4] Škorpil, V. Vysokorychlostní komunikační systémy. FEKT, Brno 2014
- [5] Pužmanová, R. Bezpečnost bezdrátové komunikace. Computer Press Books, Brno 2005. s. 1-175. ISBN:80-251-0791-4. (cs)
- [6] Maitra, A. (2003). EARLY HISTORY OF WIRELESS COMMUNICATIONS. Souvenir of 33rd Annual Convention of Radio Physics and Electronics Association, University of Calcutta.
- [7] Bayer, R. Projektování datových sítí. VUT , Brno 2019. Přednáška 1 Rozdělení počítačových sítí. (cs)
- [8] Slanina, M. Moderní bezdrátová komunikace. FEKT, Brno 2010. s. 1-164. ISBN:978- 80-214-4156-9. (cs)
- [9] Krulich, F. Bakalářská práce Pokročilý Roaming ve Wi-Fi sítích. FEKT, Brno 2019. s. 1-45. (cs)
- [10] Sekanina, T. Bakalářská práce Využití sítěWLAN pro detekci lidské aktivity uvnitř budov. FEKT, Brno 2019. s. 1-62. (cs)
- [11] Mašek, P. Doctoral Thesis Heterogenous Connectivity of Mobile Devices in 5G Wireless Systems. FEKT, Brno 2017. s. 1-164. (cs)
- [12] Wireless USB. [en.wikipedia.org](http://en.wikipedia.org) [online]. [cit. 2019-11-25].
- [13] UWB. [www.sewio.net](http://www.sewio.net) [online]. [cit. 2019-11-25].
- [14] Lojek,S. Diplomová práce Návrh laboratorních úloh v prostředí Riverbed Modeler. FEKT, Brno 2018. s. 1-108. (cs)
- [15] Přenosová rychlost. [www.wikipedie.cz](http://www.wikipedie.cz). [online]. [cit. 2019-11-25].
- [16] Největší TEST routerů 2019. [vas-pomocnik.cz](http://vas-pomocnik.cz). [online]. [cit. 2019-11-25].
- [17] BVKS, Laboratorní cvičení. Komunikační technologie Wi-Fi. FEKT, Brno 2018. s. 1-20. (cs)



- [18] Bayer, R. Projektování datových sítí. VUT, Brno 2019. Přednáška 5 Koaxiální kabely.(cs)
- [19] Bayer, R. Projektování datových sítí. VUT, Brno 2019. Přednáška 5 Kroucená dvojlinka.(cs)
- [20] Bayer, R. Projektování datových sítí. VUT, Brno 2019. Přednáška 6 Optická vlákna.(cs)
- [21] Krajíček, T. Bakalářská práce Moderní bezdrátová technologie – Zigbee. FEKT, Brno 2009. s. 1-51.(cs)
- [22] Bc. Amgalanbayar Tsevelnyam. Diplomová práce Lokalizace zařízení pomocí BLE rámců. FEKT, Brno 2017. s. 1-58.(cs)
- [23] Hlaváček, J. Diplomová práce Bezpečnostní testování zařízení s Bluetooth. FEKT, Brno 2017. s. 1-60.(cs)
- [24] Mobile Wireless Networks - Evolution, [www.pbaumgarten.com/ib-compsci/unit-3](http://www.pbaumgarten.com/ib-compsci/unit-3). [online]. [cit. 2019-11-28].
- [25] Wireless LAN, [en.wikipedia.org](http://en.wikipedia.org). [online]. [cit. 2019-11-28].
- [26] Bayer, R. Projektování datových sítí. VUT, Brno 2019. Přednáška 4 Wi-fi.(cs)
- [27] Škorpil, V. Přístupové a transportní sítě. FEKT, Brno 2012
- [28] Novotný, V. Architektura sítí. FEKT, Brno 2011
- [29] Kupka, L. Platforma pro zpracování dat z experimentální mobilní sítě LTE-A. FEKT, Brno 2017. s. 1-52.(cs)
- [30] Hlavatý, J. Bakalářská práce Návrh rozsáhlých bezdrátových sítí dle standardu IEEE 802.11. FEKT, Brno 2016. s. 1-72.(cs)
- [31] Bláha, D. Bakalářská práce Výuková pomůcka demonstrující principy WIMAX sítí. FEKT, Brno 2012. s. 1-44.(cs)
- [32] Hanus, S. Přednáška 1 Rádiové a mobilní komunikace. FEKT, Brno 2018.(cs)
- [33] Alexa, J. Bakalářská práce Ověření vlastností standardu Wifi IEEE 802.11n. FEKT, Brno 2016. s. 1-47.(cs)
- [34] Wireless network, [en.wikipedia.org](http://en.wikipedia.org). [online]. [cit. 2019-11-28].
- [35] BARS, Laboratorní cvičení. Komunikace v sítích WLAN. FEKT, Brno 2018. s. 1-7. (cs)
- [36] Security, WiFi Alliance, [wi-fi.org](http://wi-fi.org). [online]. [cit. 2019-11-29].
- [37] UWB - technology, [sewio.net](http://sewio.net). [online]. [cit. 2019-11-29].

- [38] Wi-Fi routery, TL-WR841N [www. tp-link.com](http://www.tp-link.com). [online]. [cit. 2019-11-30].
- [39] Mercusys, MW301R [www. mercusys.com](http://www.mercusys.com). [online]. [cit. 2019-11-30].
- [40] Netis, WF2411 [www. netis.cz](http://www.netis.cz). [online]. [cit. 2019-11-30].
- [41] ASUS, RT-AC1200G+ [www. asus.com](http://www.asus.com). [online]. [cit. 2019-11-30].
- [42] Inkscape, [www. inkscape.org](http://www.inkscape.org). [online]. [cit. 2019-11-30].
- [43] Picture, MERCUSYS MW301R WiFi Router, [www.discomp.cz](http://www.discomp.cz). [online]. [cit. 2019-11-30].
- [44] Picture, TP-LINK TL-WR841N, [www.amazon.in](http://www.amazon.in). [online]. [cit. 2019-11-30].
- [45] Picture, ASUS RT-AC1200G+, [www.conrad.cz](http://www.conrad.cz). [online]. [cit. 2019-11-30].
- [46] Vaněk, J. Diplomová práce Kvalita služeb a kvalita zážitku pro síť nové generace. FEKT, Brno 2018. s. 1-69. (cs)
- [47] Christian Reusch, Basics facts about WLAN standards in north America and Europe, [www.crnetspackets.com](http://www.crnetspackets.com), [online]. [cit. 2020-6-1].
- [48] 3G, [www.altaxo.cz](http://www.altaxo.cz), [online]. [cit. 2020-6-1].
- [49] Tomáš Doseděl, UMTS, HSPA+, LTE: vyznejte se v datových přenosech, [www.mobinfo.cz](http://www.mobinfo.cz), [online]. [cit. 2020-6-1].
- [50] 4G/LTE internet, [www.vodafone.cz](http://www.vodafone.cz), [online]. [cit. 2020-6-1].
- [51] Stručný průvodce technologií 4G LTE, [www.hyt.cz](http://www.hyt.cz), [online]. [cit. 2020-6-1].
- [52] What is Iperf / Iperf 3, [www.iperf.fr](http://www.iperf.fr), [online]. [cit. 2020-6-1].
- [53] Philippe Biondi and the Scapy community Revision 41862d7d, Introduction: About Scapy, [www.scapy.readthedocs.io](http://www.scapy.readthedocs.io), [online]. [cit. 2020-6-1].
- [54] Dan McInerney, wifijammer, [www.github.com](http://www.github.com), [online]. [cit. 2020-6-1].
- [55] Ing. Pavel Mašek Ph.D., Bluetooth Low Energy (BLE), BVKS, FEKT, Brno 2019.(aj)

## Seznam symbolů a zkratek

AP	–	Access Point
WiFi	–	Wireless Fidelity
IMP	–	Interface Message Processor
PAN	–	Personal Area Network
LAN	–	Local Area Network
MAN	–	Metropolitan Area Network
WAN	–	Wide Area Network
P2P	–	Peer-to-Peer
ATM	–	Asynchronous Transfer Mode
QoS	–	Quality of Service
STP	–	Shielded Twisted Pair
UTP	–	Unshielded Twisted Pair
NMT	–	Nordic Mobile Telephone
AMPS	–	Analog Mobile Phone System
TACS	–	Total Access Communication System
1G	–	First Generation of Wireless Cellular Technology
2G	–	Second Generation Cellular Technology
2,5G	–	Second and Half Generation of Technology
3G	–	Third Generation of Wireless Mobile Technology
4G	–	Fourth Generation of Broadband Cellular Network Technology
5G	–	Fifth Generation of Cellular Network Technology
GSM	–	Global System for Mobile Communications
TDMA	–	Time Division Multiple Access

FDMA	–	Frequency Division Multiple Access
CDPD	–	Cellular Digital Packet Data
CDMA	–	Code Division Multiple Access
GPRS	–	General Packet Radio Service
EDGE	–	Enhanced Data Rates for GSM Evolution
UMTS	–	Universal Mobile Telecommunication System
BSC	–	Binary Synchronous Communication
HSPA	–	High Speed Packet Access
HSDPA	–	High Speed Downlink Packet Access
HSUPA	–	High Speed Uplink Packet Access
MIMO	–	Multiple Input, Multiple-Output
LTE	–	Long Term Evolution
EPC	–	Evolved Packet Core
UTRAN	–	Universal Terrestrial Radio Access Network
MME	–	Mobility Management Entity
UWB	–	Ultra-Wideband
FHSS	–	Frequency Hopping Spread Spectrum
AFH	–	Adaptive Frequency Hopping
RSSI	–	Received Signal Strength Indication
EDR	–	Enhanced Data Rate
MAC	–	Media Access Control
OFDM	–	Orthogonal Frequency Division Multiplexing
RCN	–	Radio Network Controller
PDN	–	Public Data Network
QPSK	–	Quadrature Phase Shift Keying

IP	–	IP Address
3GPP	–	The 3rd Generation Partnership Project
WLAN	–	Wireless LAN
WPA	–	Wi-Fi Protected Access
MU-MIMO	–	Multiple-User Multiple-Input Multiple-Output
BSSID	–	Basic Service Set Identifiers
SSID	–	Service Set Identifier
HiperLAN	–	High Performance Radio LAN
EDCF	–	Enhanced Distribution Coordination Function
SLA	–	Service Level Agreement
AIFS	–	Arbitration Interframe Space
HCCA – HCF	–	Controlled Channel Access
ISO/OSI	–	OSI Reference Model
IEEE	–	Institute of Electrical and Electronics Engineers
DSSS	–	Direct-Sequence Spread Spectrum
CSMA/CA	–	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	–	Carrier Sense Multiple Access with Collision Detection
SC	–	Single Carrier
DoS	–	Disk Operating System
ESSID	–	Extended Service Set Identification
WEP	–	Wired Equivalent Privacy
PSK	–	Pre-Shared Key
CCMP	–	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
AES	–	Advanced Encryption Standard

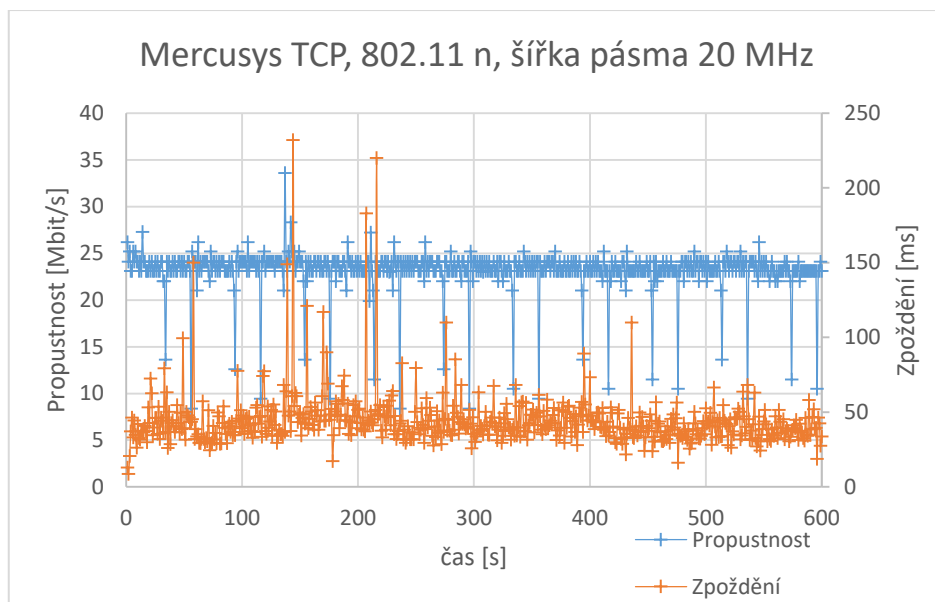
PMF	–	Protected Management Frames
SHA	–	Secure Hash Algorithm
SAE	–	System Architecture Evolution
GCMP	–	Galois/Counter Mode
HMAC	–	Hash-based Message Authentication Code
ECDH	–	Elliptic-curve Diffie-Hellman
WHO	–	World Health Organization
IARC	–	International Agency of Research on Cancer
HPA	–	Health Protect Agency
IPX/SPX	–	Internetwork Packet Exchange / Sequenced Packet Exchange
HD	–	High Definition
SVG	–	Scalable Vector Graphics
W3C	–	World Wide Web Consortium
PDF	–	Portable Document Format
PS	–	PostScript
PNG	–	Portable Network Graphics
SVG	–	Scalable Vector Graphics
AI	–	Adobe Illustrator
EPS	–	Encapsulated PostScript
RPi	–	Raspberry Pi

## Seznam příloh

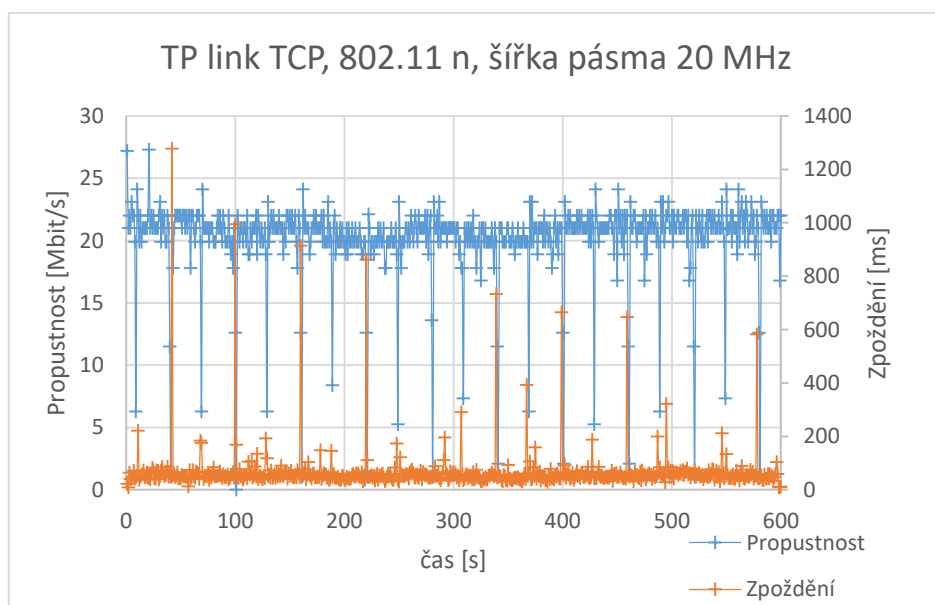
Příloha 1 - Naměřené průběhy .....	80
Příloha 2 - Manuál pro vyučující / studenty .....	86
Příloha 3 - Manuál pro vyučující / studenty .....	96
Příloha 4 - Vzorový protokol .....	115
Příloha 5 - Vzorový protokol č.2 .....	120
Příloha 5a - Popis routeru Mercusys MW301R .....	122
Příloha 5b – Popis routeru TP - LINK model TL-WR841N .....	123
Příloha 5c – Popis routeru Netis WF2411 .....	124
Příloha 5d – Popis routeru ASUS RT-AC1200G+ .....	125
Příloha 5e - Souhrn parametrů routerů použitých při měření .....	126

# Příloha 1 - Naměřené průběhy

Ověření parametrů přenosu s RPi Zero

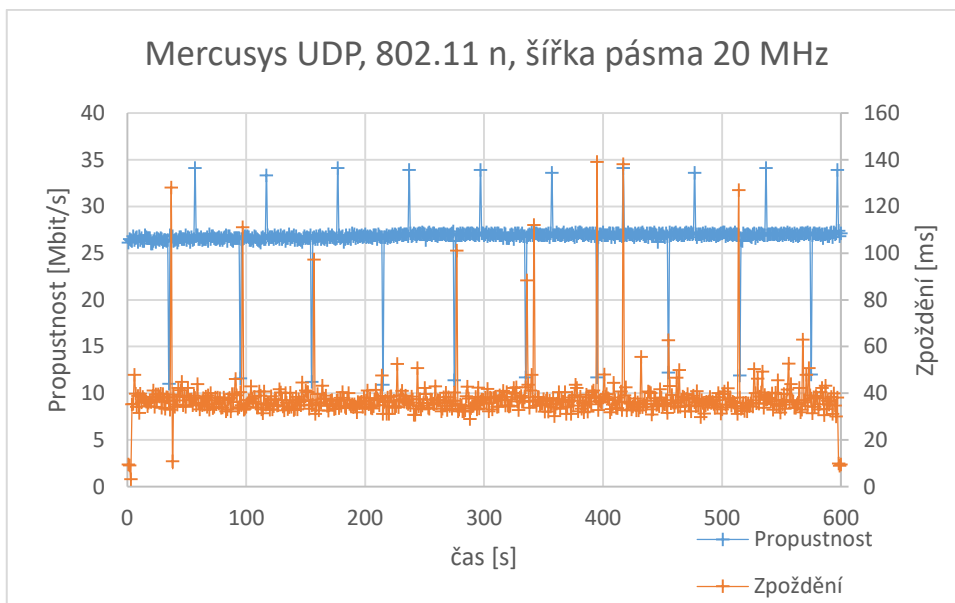


Obr. 1.13: Přenos TCP pro router Mercusys s použitým standardem 802.11 n

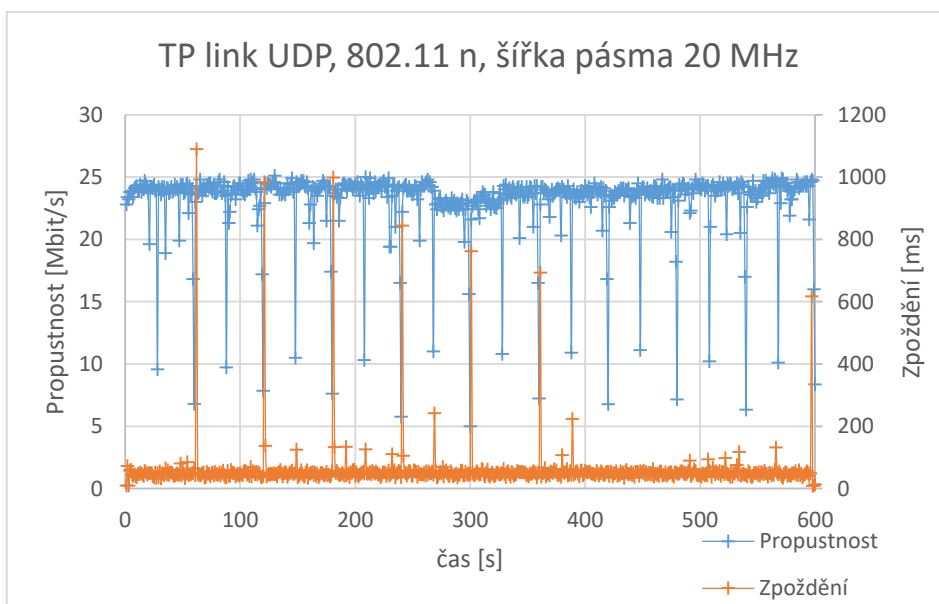


Obr. 1.14: Přenos TCP pro router TP-Link s použitým standardem 802.11 n



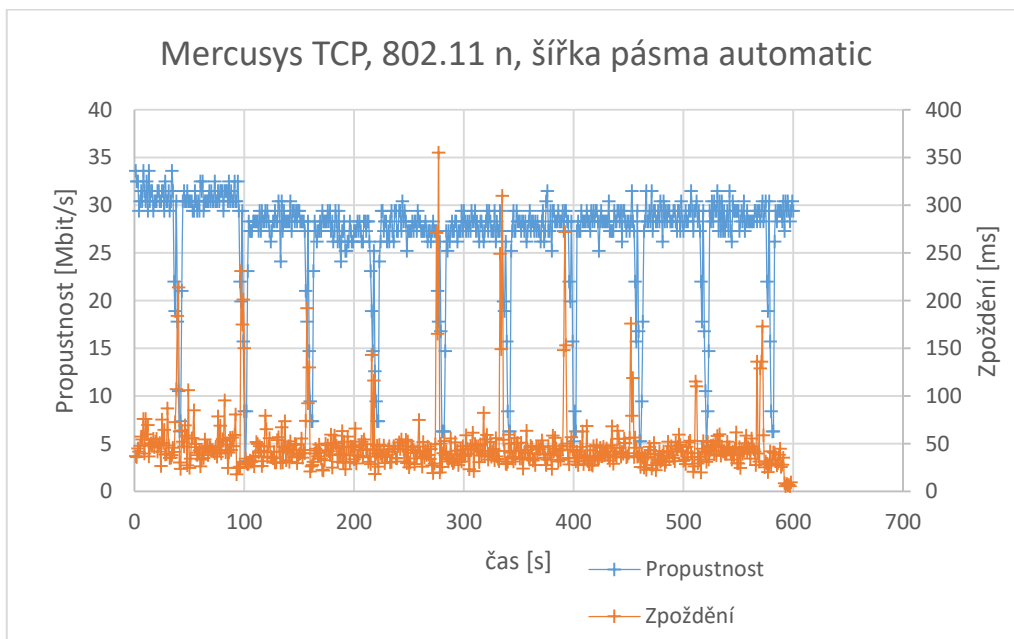


Obr. 1.15: Přenos UDP pro router Mercusys s použitým standardem 802.11 n

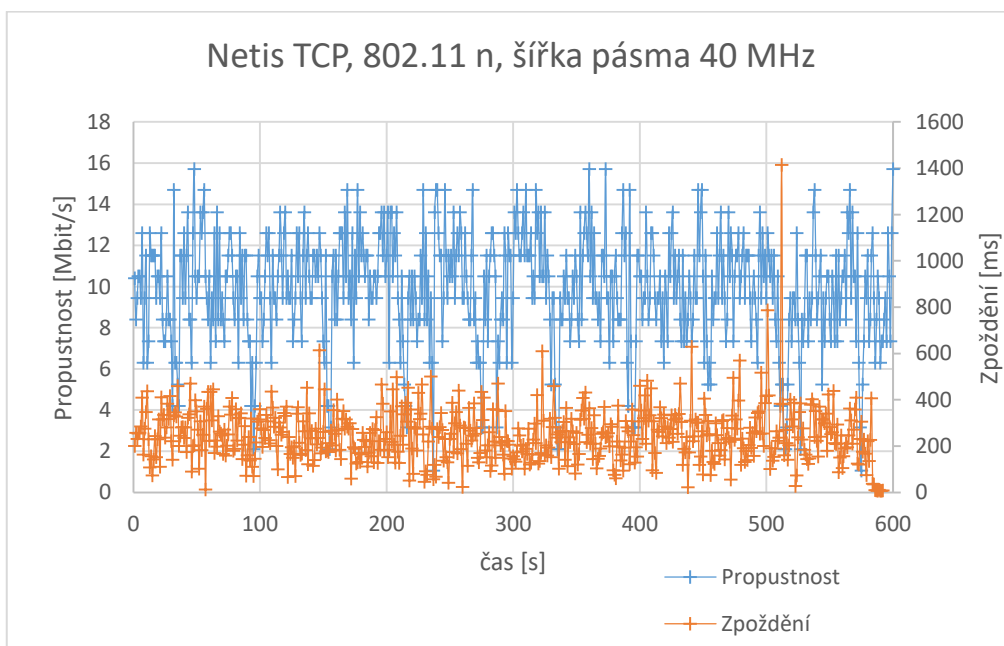


Obr. 1.16: Přenos UDP pro router TP-Link s použitým standardem 802.11 n

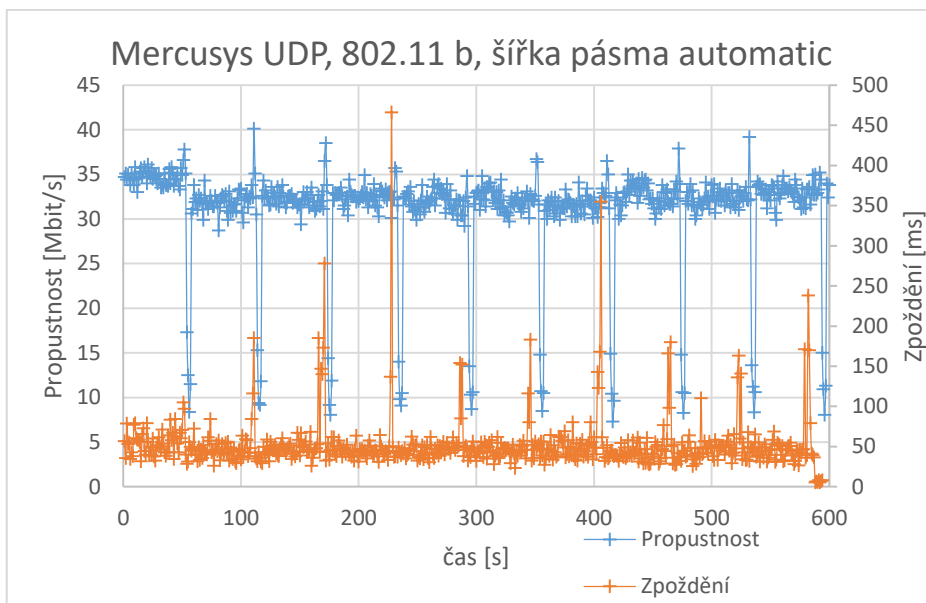
## Ověření parametrů přenosu s RPi 4



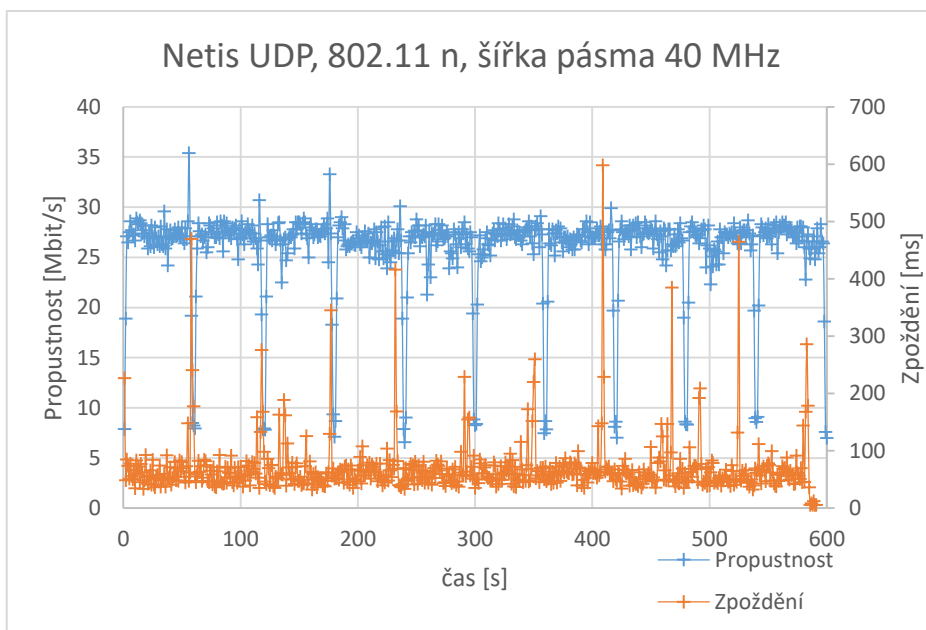
Obr. 1.17: Přenos TCP pro router Mercusy s použitým standardem 802.11 n



Obr. 1.18: Přenos TCP pro router Netis s použitým standardem 802.11 n

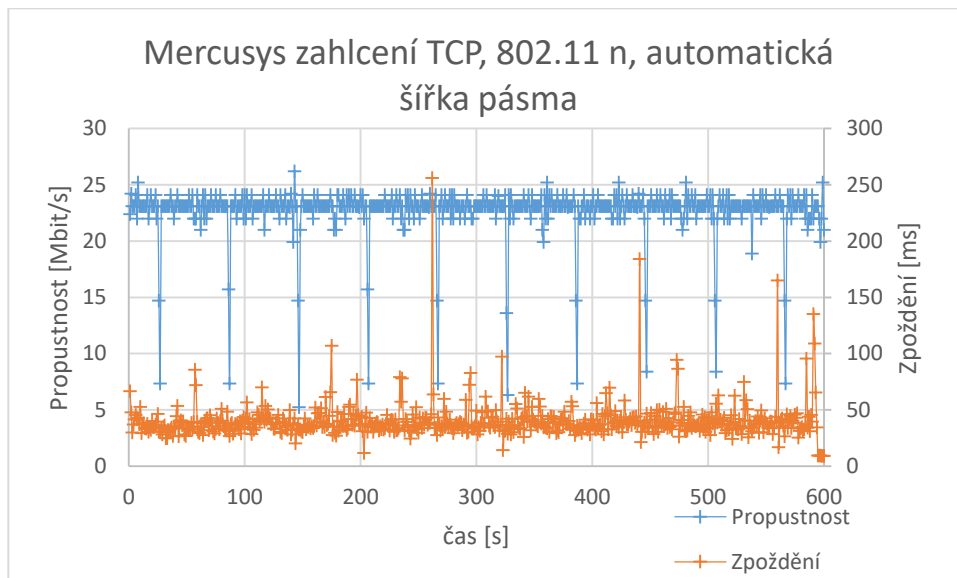


Obr. 1.19: Přenos UDP pro router Mercusys s použitým standardem 802.11 n

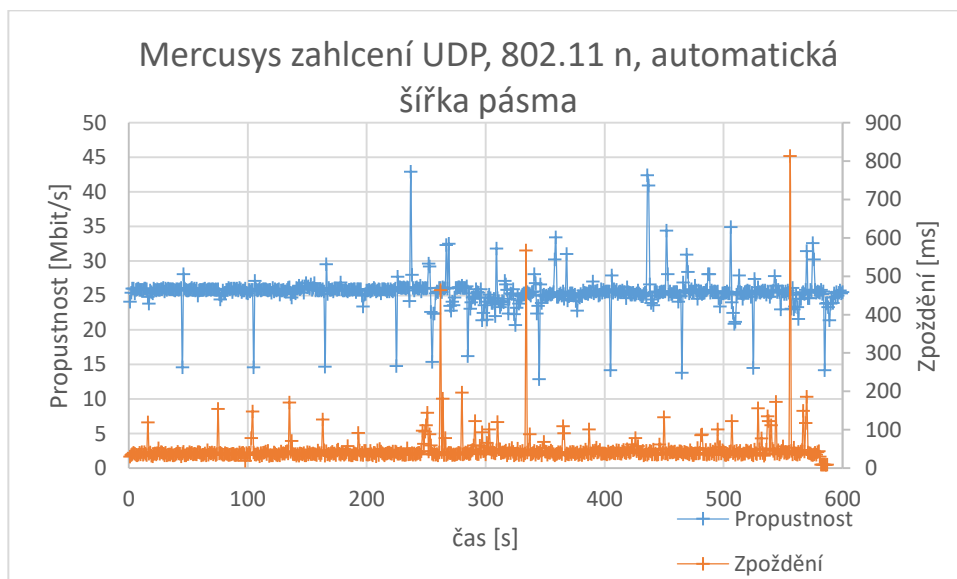


Obr. 1.20: Přenos UDP pro router Netis s použitým standardem 802.11 n

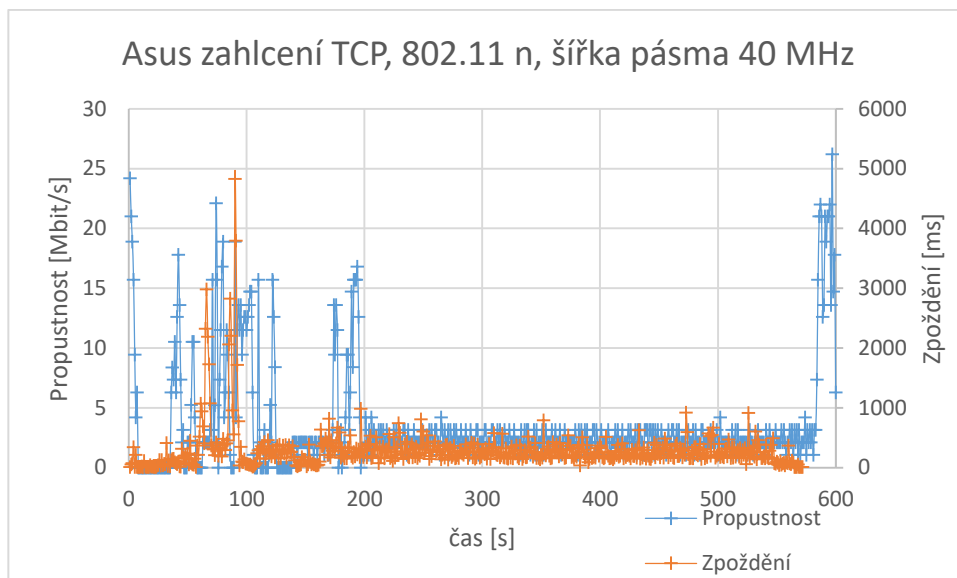
Zahlčení pomocí skriptu wifijammer



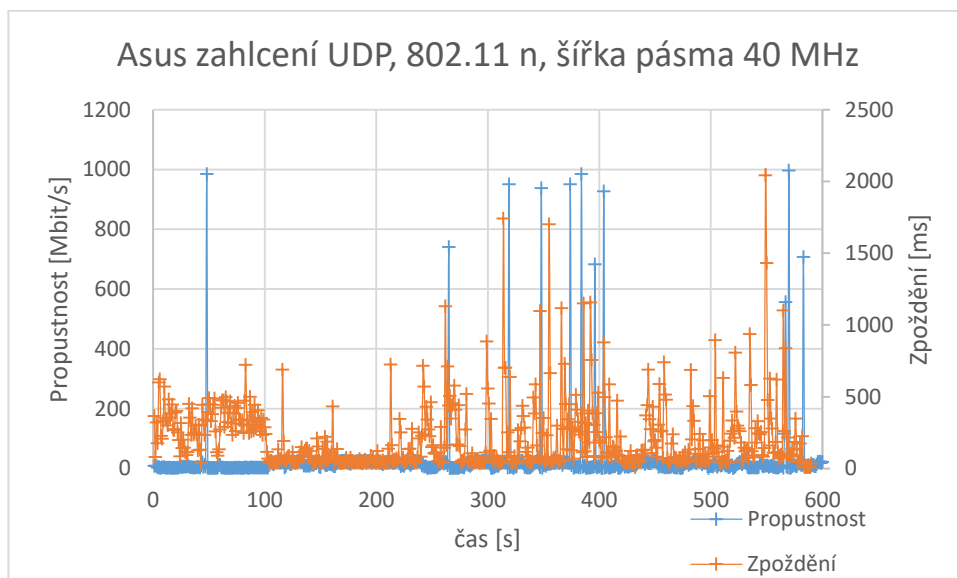
Obr. 1.21: Přenos TCP pro router Mercusys s použitým standardem 802.11 n



Obr. 1.22: Přenos UDP pro router Mercusys s použitým standardem 802.11 n



Obr. 1.23: Přenos TCP pro router Asus s použitým standardem 802.11 n



Obr. 1.24: Přenos UDP pro router Asus s použitým standardem 802.11 n

## Příloha 2 - Manuál pro vyučující / studenty

Přístupové a transportní sítě

Laboratorní úloha

### **Vzájemné testování WLAN sítí v pásmu 2,4 GHz**

V této laboratorní úloze se budete věnovat problematice rušení WLAN sítí v pásmu 2,4GHz, které má způsobit horší příjem signálu Wi-Fi routeru Mercusys.

Cílem úlohy je prostudovat vliv rušení v pásmu 2,4 GHz nastavením vhodného standardu, kanálu pásma, vysílacího výkonu a přenosové rychlosti.

V úloze se budete zabývat konfigurací jednotlivých prvků sítě, tak aby dosaženo požadovaného rušení.

### **Teoretický úvod**

V dnešní době jsou standardy 802.11n a 802.11ac považovány za nejužívanější, co se bezdrátové komunikace týče. Standard 802.11n a 802.11ac využívají modulaci OFDM, díky které je dosaženo mnohem vyšší přenosové rychlosti, neboť umožňuje rozšíření šířky kmitočtového pásma. Standard 802.11n využívá šířku pásma až 40 MHz a standard 802.11ac až 160 MHz. Oba dva standardy podporují přenosovou techniku MIMO. Standard 802.11ac ji později ještě rozšířil na MU-MIMO. S modulací 64-QAM pracuje standard 802.11n. Druhý zmíněný standard 802.11ac využívá modulaci 256-QAM. Teoretický dosah ve venkovním prostředí je pro standard 802.11n 250m a ve vnitřním prostředí 70m. U standardu 802.11ac je teoretický dosah poloviční. Dříve byly hojně využívány standardy 802.11a, 802.11b a 802.11g. Standard 802.11a dokáže pracovat pouze v pásmu 5 GHz, což pro tento standard představuje mnoho výhod, ale nevýhod. Přenosová rychlost dosahuje až 54 Mbit/s. Nedokáže však komunikovat se staršími zařízeními v pásmu 2,4 GHz. Standard 802.11b pracuje v pásmu 2,4 GHz a proto je brán jako pokračování předchozího standardu 802.11a. Dokáže komunikovat i se zařízeními v pásmu 2,4 GHz. Dosahuje již menší přenosové rychlosti oproti standardu 802.11a a tedy 11 Mbit/s. Oproti předchozím standardům využívá modulaci DSSS. Standard

802.11g pracuje v pásmu 2,4 GHz a využívá stejnou modulaci OFDM jako standard 802.11a. Dosahuje přenosové rychlosti 54 Mbit/s.

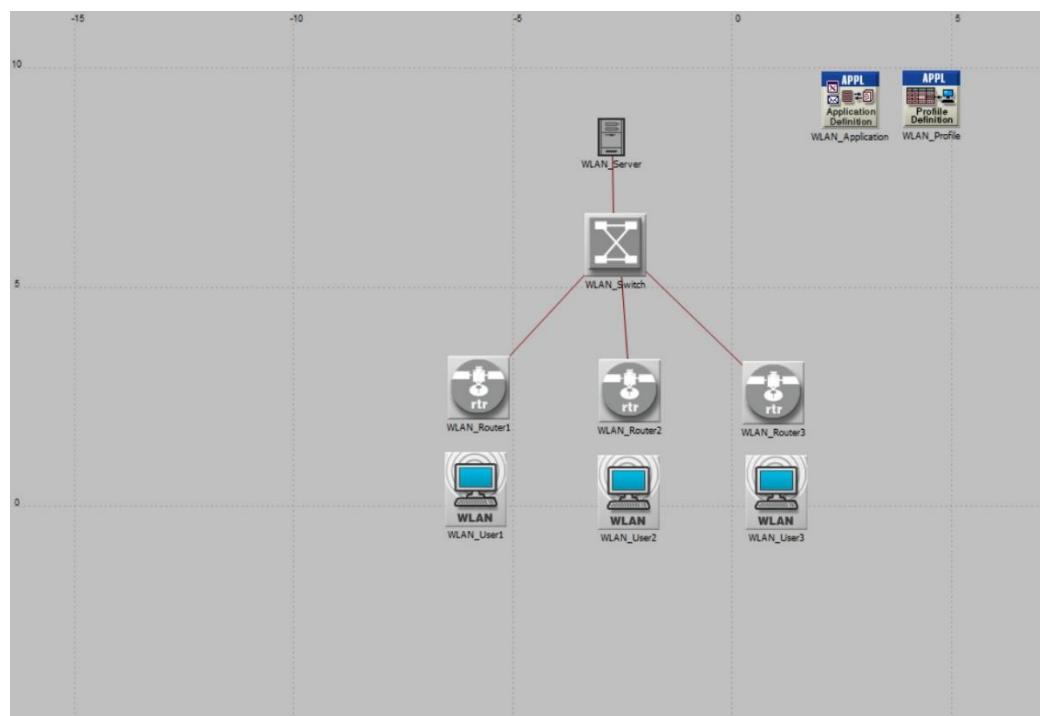
V úloze se nastavením parametrů na WLAN routerech bude v programu Riverbed zkoumat vliv rušení v pásmu 2,4 GHz. Parametry, které ovlivňují rušení, se nastaví podle tabulky 1. Pro rušení WLAN je důležité si uvědomit, že je nutné nastavit potřebné parametry jako vysílací výkon, pásmo a přenosovou rychlost a v neposlední řadě vybrat vhodný standard. Pro úlohu je nejvhodnější standard 802.11g, který podporuje pouze pásmo 2,4 GHz a přenosovou rychlost 54Mbit/s. Blokové schéma zapojení pracoviště je zobrazené na Obr. 1.

Nastavené parametry pro pásmo 2,4 GHz u standardu 802.11g je barevně vyznačeno.

IEEE standard	Rok založení standardu	Kmitočtové pásmo [GHz]	Šířka pásma 1. kanálu [MHz]	Max. přenosová rychlost [Mbit/s]	Modulace
802.11	1997	2,4	22	2	DSSS, FHSS
802.11a	1999	5	20	54	OFDM
802.11b	1999	2,4	22	11	DSSS
802.11g	2003	2,4	20	54	DSSS, OFDM
802.11n	2009	2,4 nebo 5	20   40	600	OFDM
802.11ac	2013	5	20   40   80   160	6933	OFDM
802.11ad	2012	60	2160	6756	OFDM
802.11af	2014	0,54 až 0,79	6   7   8	26,7	OFDM
802.11ah	2016	0,9	1   2   4   8   16	40	OFDM
802.11ax	2019	2,4 nebo 5	20   40   80   160	9607,8	OFDM, OFDMA

Tab. 1.1: Srovnání jednotlivých standardů

Schéma zapojení v programu Riverbed Modeler Academic Edition 17,5



Obr. 1.3: Schéma zapojení vzájemného ovlivnění WLAN sítí

## Úkoly

1. Sestrojte topologii v programu Riverbed dle zadání.
2. Nakonfigurujte jednotlivé prvky v zadání dle pokynů.
3. Zobrazte výsledné grafy v programu Riverbed a tyto grafy okomentujte v závěru.

## Zadání a postup měření

1. Pokud je počítač na pracovišti spuštěn, tak kliknutím na ikonu programu Riverbed tento program spustíte a sestavíte zapojení podle schématu v návodu úlohy.

### Postup:

Seznamte se s programem Riverbed. V programu Riverbed v položce File => Manage model files => Add model directory. V novém okně se přepne na záložku Plocha (desktop). Zde v dokumentech => downloads => vytvoříte Riverbed project. Složku označíte a potvrdíte tlačítkem Ok. V okně Confirm model directory označíte možnost Make this the default directory a potvrdíte Ok. Pokud program projekt nedovolí uložit, je to způsobeno tím, že již projekt stejného názvu existuje a je nutné jej pozměnit. V záložce File => New => Project vytvoříte nový projekt a potvrdíte tlačítkem OK. Zobrazí se okno, kde projekt pojmenujete jako WLAN test. Vše ostatní ponecháme beze změny. A potvrdíte opět tlačítkem OK. Zobrazí se dialog Initial Topology, kde zvolíte Create empty scenario. A potvrdíte tlačítkem NEXT. V dialogu Choose network scale zvolíte možnost Campus, vše ostatní ponecháte beze změny. V dialogu Specify Size změníte nastavení na X span: 20, Y span: 20, Units: Meters. Potvrdíte tlačítkem NEXT. V dialogu Select Technologies zvolíte wireless\_lan a wireless\_lan\_adv. Potvrdíte tlačítkem NEXT. V dialogu Review zkontrolujete vámi vybrané parametry a potvrdíte tlačítkem FINISH. Podle schématu v návodu úlohy sestavíte zapojení. Dodržujte výběr komponent.

Z palety na ploše Object Palette Tree vyberete 3x wlan2\_ethernet\_router\_adv Fixed Node, přepínač ethernet16\_switch Fixed Node, ethernet\_server Fixed Node, 3x wlan\_wkstn\_adv Fixed Node, Application Config, Profile Config a linku 100BaseT. Komponenty ethernet\_server a ethernet16\_switch jsou propojeny linkou 100BaseT k jednotlivým routerům. Propojení začněte od komponenty ethernet\_server ke komponentě ethernet16\_switch a jednotlivé routery propojte ke komponentě WLAN\_Switch. Komponenty pojmenujte podle obrázku v zadání. Pojmenování se provádí pravým kliknutím na vybranou komponentu a zvolením Set Name.



2. Pro nastavení parametrů routerů WLAN\_Router1, WLAN\_Router2 a WLAN\_Router3 na ně kliknete pravým tlačítkem na myši. Otevře se lišta, kde vyberete Edit Attributes.

Postup:

Klikněte pravým tlačítkem na komponentu wlan2\_ethernet\_router\_adv pojmenovanou jako WLAN\_Router1. Pro nastavení všech důležitých parametrů je důležité, abyste vybrali Edit Attributes. Zde se zobrazí jednotlivá nastavení pro router WLAN\_Router1. Kliknete na záložku Wireless LAN a po rozkliknutí se zobrazí Wireless LAN Parameters, kde nastavíte hodnotu BSS Identifier na 1. Nastavení potvrdíte tlačítkem Ok. Totéž provedete pro WLAN\_Router2, kde ale nastavíte hodnotu BSS Identifier na 2. A stejným postupem, jako v případě routeru WLAN\_Router1, nastavíte hodnotu BSS Identifier u WLAN\_Router3 na hodnotu 3.

3. Pro nastavení pracovních stanic, neboli workstations, musíte opět jít ze známého nastavení přes výběr Edit Attributes.

Postup:

Po nastavení jednotlivých routerů musíte nastavit parametry pro wlan\_wkstn\_adv. Opět pravým kliknete na vybranou komponentu workstation, pojmenovanou jako WLAN\_User1 a zobrazí se lišta Edit Attributes. V položce Wireless LAN Parameters zvolíte hodnotu BSS Identifier tak, aby odpovídala routeru nad danou stanicí. Pro WLAN\_User1 tato hodnota bude nastavená na 1. Pro WLAN\_User2 bude nastavená na hodnotu 2 a pro WLAN\_User3 na hodnotu 3.

4. Pro nastavení standardu a přenosové rychlosti musíte do nastavení v horní liště s názvem Protocols.

Postup:

V liště Protocols zvolíte možnost Wireless LAN => Configure PHY and Data Rate. Objeví se lišta, ve které se dá jednoduše zvolit standard a přenosová rychlost. Pro vzájemné ovlivnění WLAN sítí je vhodné vybrat standard, který podporuje pásmo 2,4 GHz a nejnižší možnou přenosovou rychlost, kterou standard nabízí. Standard 802.11b pracuje v pásmu 2,4 GHz a nabízí přenosovou rychlost 11 Mbit/s. Program Riverbed automaticky nabízí tento standard a není tedy nutné nic měnit. Výběr a nastavení potvrdíte tlačítkem Ok.

5. Pro nastavení parametrů Application Config a Profile Config je konfigurace složitější.

Postup:

Pravým tlačítkem kliknete na komponentu pojmenovanou jako WLAN\_Application. Zobrazí se lišta, ve které zvolíte Edit Attributes. V položce Application Definitions zvolíte hodnotu Number of Rows na Default. Konfigurace komponenty WLAN\_Profile provedete kliknutím pravým na tuto komponentu, kde se zobrazí lišta, ve které zvolíte Edit Attributes. V záložce Profile Configuration nastavíte hodnotu Number of Rows na 1. Zobrazí se lišta, ve které v řádku Enter Profile Name vyplníte název wlan\_testing. V záložce Application do hodnoty Rows napíšete 1 a zobrazí se vám další lišta, kde zvolíte možnost File Transfer Heavy. Vše ostatní ponecháte beze změny a vybrané parametry potvrdíte tlačítkem Ok. V liště (Profile Configuration) Table je vše již nastaveno a proto toto nastavení měnit již nebudete a jenom potvrdíte tlačítkem Ok. Celou konfiguraci zavřete tlačítkem Ok. Poté označíte všechny tři stanice a pravým kliknutím vstoupíte do jejich konfigurace. V záložce Application: Supported Profiles nastavíte hodnotu Number of Rows na 1. Objeví se řádek, na kterém je napsáno, Profile Name. Po rozkliknutí nabízí možnost již předem vámi vytvořeného profilu wlan\_testing. Vše potvrdíte Ok. V liště Attributes zaškrtnete možnost Apply to selected objects. Vše poté potvrdíte tlačítkem Ok.

6. Poslední konfiguraci provedete pro komponentu server.

Postup:

Pro konfiguraci serveru s názvem ethernet\_server opět pravým tlačítkem kliknete na vybranou komponentu a zvolíte možnost Edit Attributes. V záložce Application: Supported Services nastavíte hodnotu Number of Rows na 1. V záložce Name zvolíte možnost File Transfer Heavy. Ostatní nastavení ponecháte beze změny. Vše potvrdíte tlačítkem Ok.

## 7. Zobrazení statistik a grafů v programu Riverbed.

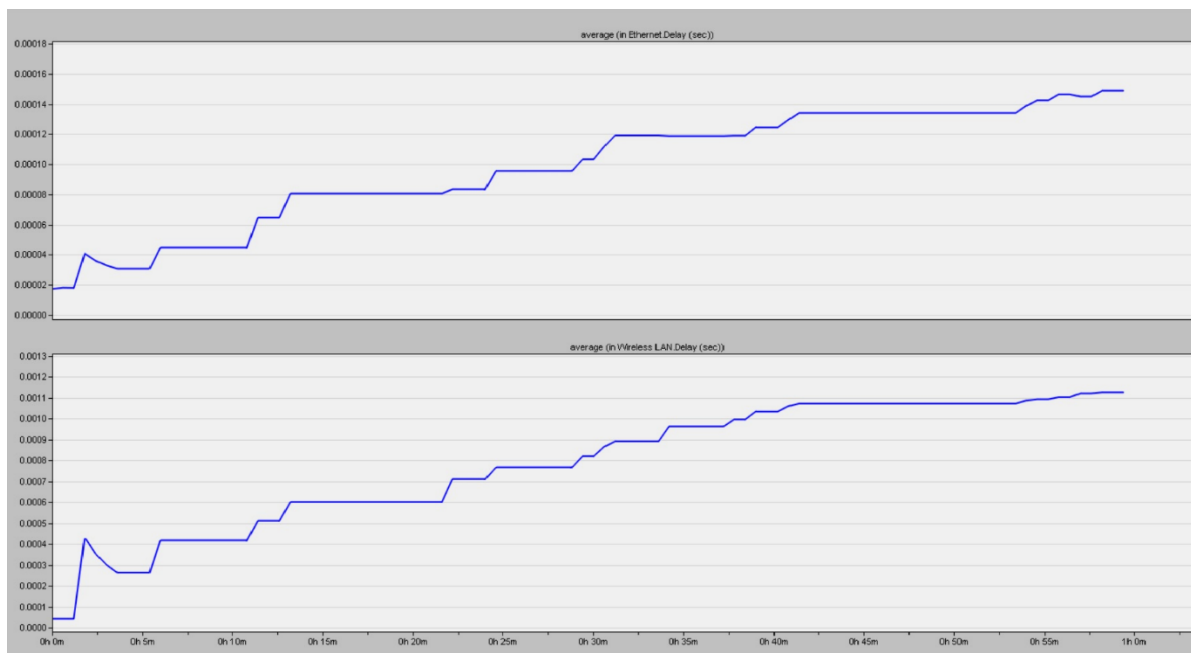
### Postup:

Pro nastavení vybraných statistik pravým tlačítkem kliknete na plochu na libovolné místo a v zobrazené liště zvolíte možnost Choose Individual DES Statistics. Zobrazí se lišta Choose Result, ve které navolíte statistiky, které chcete sledovat. V záložce Global Statistics vyberete možnost Ethernet => Delay (sec). V záložce Global Statistics je nutné ještě označit Wireless LAN, kde také označíte Delay (sec). V horní liště zvolíte Run. Duration nastavíte na 1 hodinu a Values per statistics nastavíte na 100. Poté stisknete tlačítko RUN. Objeví se lišta Simulation Progress: wlan\_testing – Scenario, kde se dá sledovat průběh simulace. Až simulace doběhne, zobrazí se Simulation Completed. Vše zavřete a v horní záložce Result Browser se vám zobrazí výsledné grafy z měření. Ze záložky DES Graphs zvolíte Results for: Current Scenario. V záložce Global statistics vyberete možnost grafu pro Delay (sec). V záložce Presentation zvolíte možnost Stacked Statistics a average pro přehlednost zobrazení výsledného grafu. Pro nastavení statistiky Throughput (bits/sec) je nutné kliknout na plochu pravým tlačítkem a vybrat možnost Choose Individual DES Statistics. V liště Choose Result klikneme na záložku Global Statistics => Wireless LAN => Throughput (bits/sec). Dále zvolíme v liště Node Statistics => Wireless LAN => Throughput (bits/sec). Poté je nutné nastavení uložit a spustit simulaci nastavenou na 1 hodinu a Values per statistics na hodnotu 100. Po skončení simulace klikneme v horní liště na View Results a zobrazí se nám lišta Results Browser. Zde vybereme možnost Current Scenario a námi vytvořený project. Poté klikneme na Global Statistics => Wireless LAN => zatrhneme možnost Throughput (bits/sec). Tím se nám zobrazí graf zahazování Throughput (bits/sec). Pro přehlednost je lepší vždy zobrazovat pouze jednotlivé grafy. To docílíme tlačítkem Show ve spodní části pravé strany obrazovky. Grafy ukládáme na flash disk, nebo pomocí printscreen.

## 8. Výsledné grafy

### Postup:

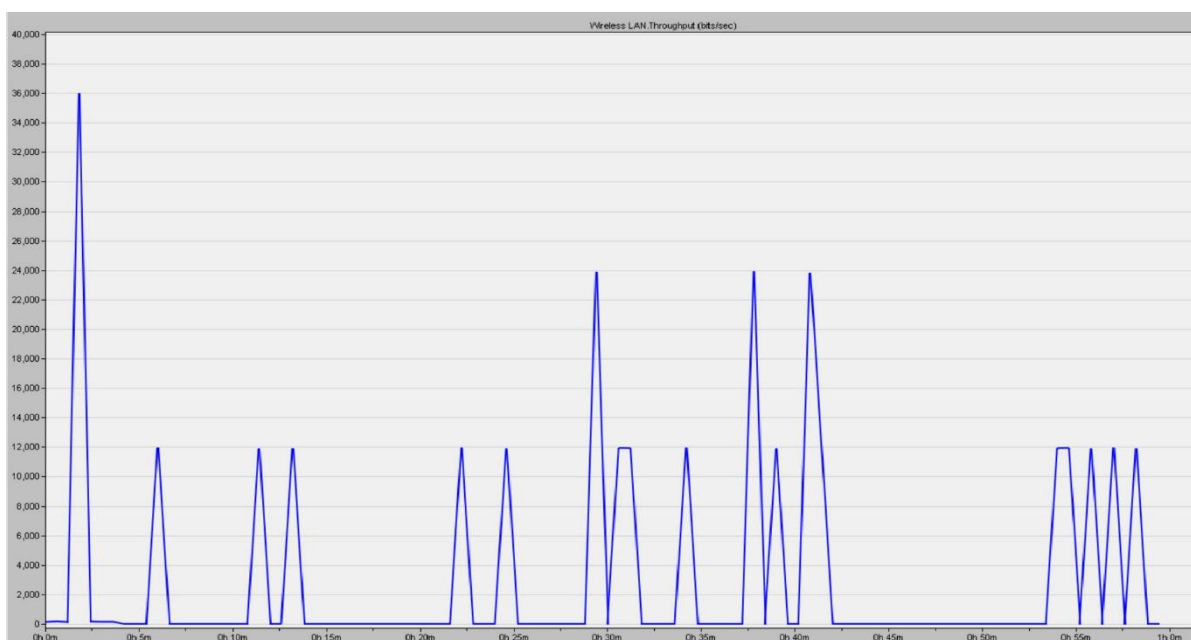
Zobrazený graf wlan\_testing Delay (sec) nám poukazuje na to, že docházelo k postupnému nárůstu zpoždění při přenosu dat při nastavení standardu 802.11g.



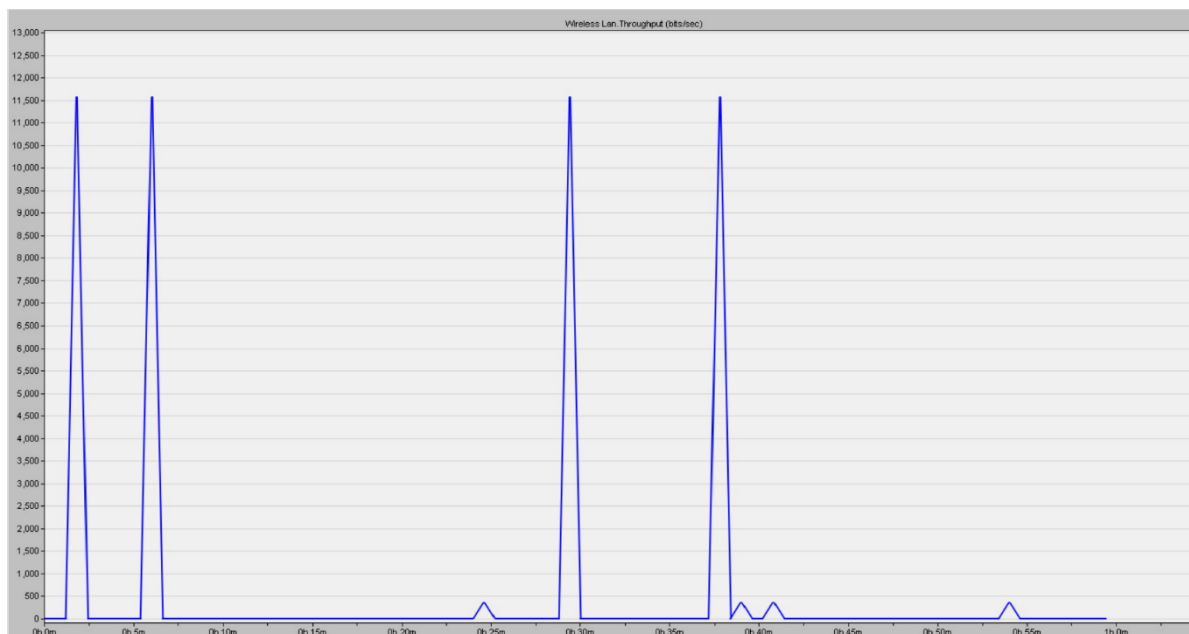
Obr. 1.8: WLAN zpoždění

Zobrazený graf wlan\_testing Throughput (bits/sec) nám naopak poukazuje na to, že docházelo ke snížení/zvýšení propustnosti při přenosu dat při nastavení standardu 802.11g

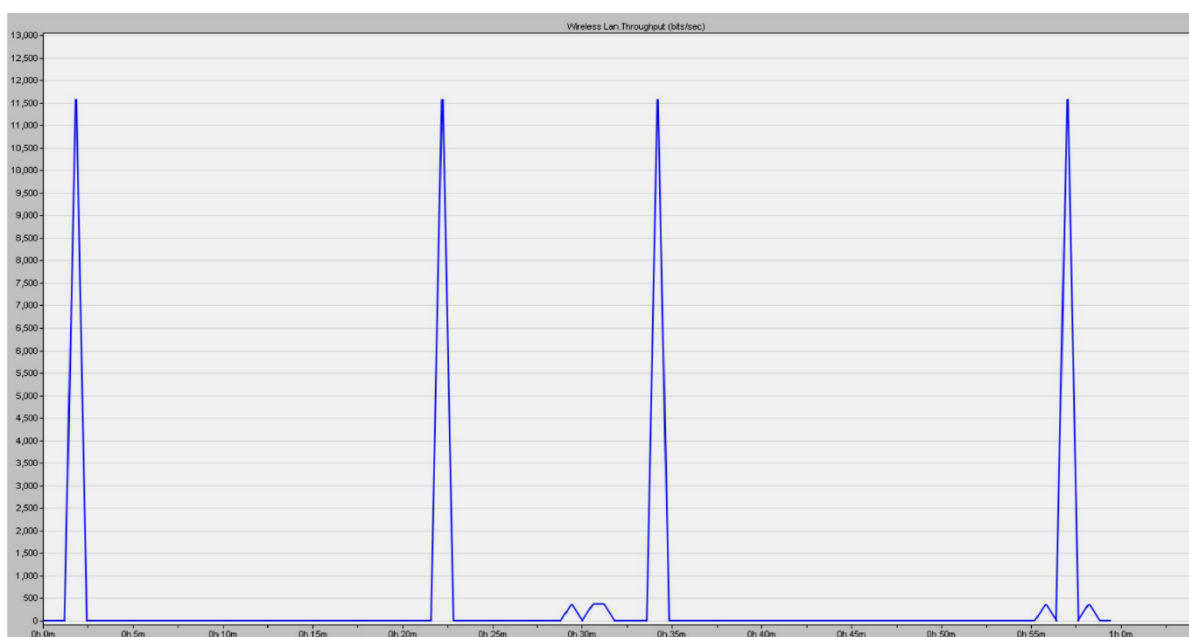
Zobrazení propustnosti pro jednotlivé routery



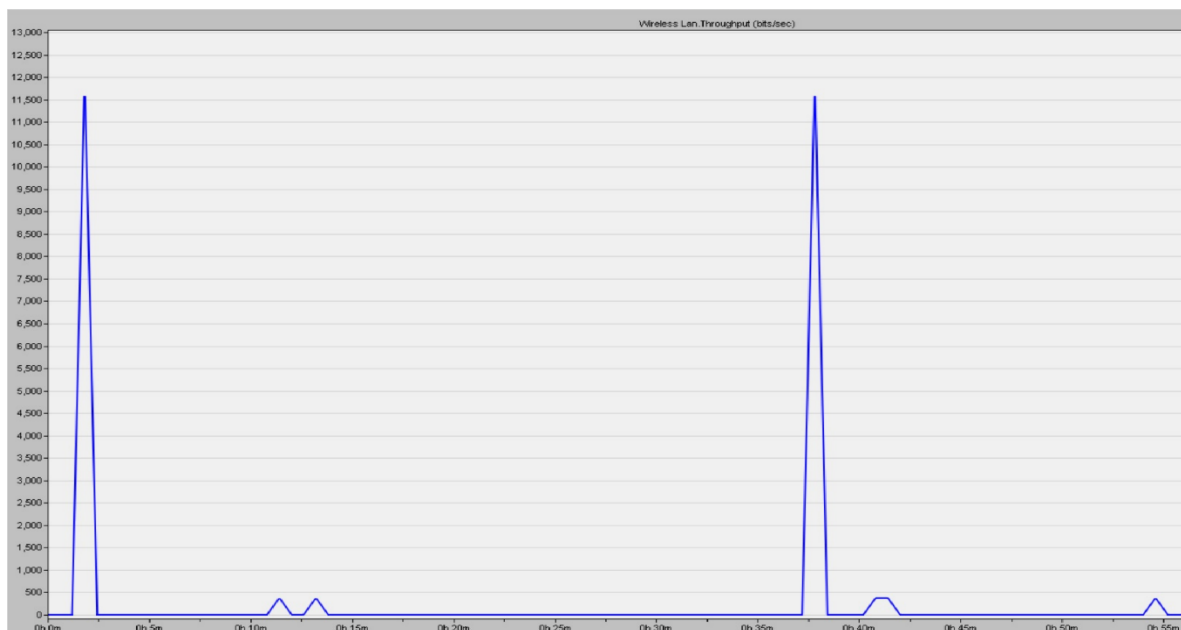
Obr.1.4: Celková propustnost 1



Obr. 1.5: Propustnost Routeru 1



Obr. 1.6: Propustnost Routeru 2



Obr.1.7: Propustnost routeru 3

## Použité přístroje

Pc s nainstalovaným programem Riverbed

SW topologie se serverem a switchem propojených linkou 100 BaseT, třemi routery WLAN a třemi počítači.

## Závěr měření

Do závěru každý student zhodnotí body měření podle postupu v zadání. Komentuje vzniklé grafické průběhy v závislosti na vzájemném ovlivňování WLAN sítí. Zhodnoďte také, zda se výsledky shodují s teoretickými předpoklady. Zmiňte problémy, které se objevily během měření.

## Kontrolní otázky

1. Proč je použit standard 802.11g?
2. Záleží na umístění jednotlivých routerů (v přímce, kruhově, atd.), anebo na jejich rozmístění nezáleží?
3. Co by se stalo, kdyby byly použity WLAN routery s pásmem 5 GHz a jaký vliv by to mělo na dosah signálu?

## **Odpovědi na kontrolní otázky**

- 1) Standard 802.11g je zde využit kvůli jeho maximální přenosové rychlosti 54 Mbit/s a také pro jeho možnost využití pásma 2,4 GHz, ve kterém dochází k ovlivňování WLAN, neboť v tomto pásmu pracují nejenom routery, ale i zařízení jako mikrovlnné trouby, Bluetooth, apod.
- 2) Na rozmístění jednotlivých routerů záleží. Jinak se budou ovlivňovat routery umístěné do kruhu a jinak se budou ovlivňovat routery umístěné do přímky.
- 3) 5 GHz pásmo není tolik zahlcené jako pásmo 2,4 GHz. Zlepšila by se nejen rychlost připojení a přenosu dat. Síla signálu u 5 GHz by se však zmenšila, pokud by v cestě stály překážky (zdi, dveře, skříně,...).

## **Použitá a doporučená literatura**

- [1] JEŘÁBEK, J. Komunikační technologie. Brno: Vysoké učení technické v Brně, 2019. s. 1-175. ISBN: 978-80-214-4713-4. (cs)
- [2] BVKS, Laboratorní cvičení. Komunikační technologie Wi-Fi. FEKT, Brno 2018. s. 1-20. (cs)
- [3] BARS, Laboratorní cvičení. Komunikace v sítích WLAN. FEKT, Brno 2018. s. 1-7. (cs)

## Příloha 3 - Manuál pro vyučující / studenty

Přístupové a transportní sítě

Laboratorní úloha

**Vzájemné rušení WLAN sítí**

### Teoretický úvod

Ve stejném roce jako vznikl standard IEEE 802.11 a vznikl i standard 802.11 b, který pracuje ve stejném pásmu a má i tu samou šířku kanálu jako 802.11 a. Pro přenos využívá DSSS modulaci na fyzické vrstvě. Tento standard byl spíše takovým pokračováním standardu 802.11a než, že by přinesl něco převratného. Co bylo u tohoto standardu nové, je interoperabilita se zastaralými médii, kterou doplňuje pro 802.11a.

802.11n výrazně posunul technologii WLAN dopředu. Jedna z jeho výhod je použití pásma 2,4 GHz tak i pásma 5 GHz, šířka kanálu může být 20 MHz anebo 40 MHz. Na fyzické vrstvě se používá modulační technika OFDM a nově je zde přenosová rychlost posunuta až na 300Mbit/s. Novinkou je zde i technologie MIMO (multiple-input multiple-output). Ta dává možnost využít v rádiovém kanálu více antén, které mohly vytvořit více datových toků ve stejném pásmu a díky tomu se může dosáhnout i větší přenosové rychlosti. Tento standard pro bezdrátové technologie byl jako první schopen konkurence před technologií Fast Ethernet. Nevýhodou bylo, že kvůli možnosti rozšíření šířky pásma z 20 na 40 MHz nastaly problémy s interferencí v pásmu 2,4 GHz a proto by se tato možnost měla využívat pouze tehdy, pokud bude jisté, že nebude ovlivňovat žádné další bezdrátové technologie ve svém okolí jako je Zigbee nebo Bluetooth. Tato možnost rozšíření pásma je proto pro 5 GHz pásmo omezena. Celé testování využívá program Scapy a skript wifijammer, které umí zahlcovat síť a tedy způsobit její výpadky nebo rušení. Scapy je program psaný v programovacím jazyce Python. Program Scapy je interaktivní výkonný program, který manipuluje s pakety (odesílá je a přijímá ve formě odpovědí). Má také schopnost, která umožňuje snímání, skenování nebo útočení na síť. Velice často nahrazuje hping, arpspoof, arp-sk, arping,



p0f a dokonce i některé části Nmap, tcpdump a tshark. Pro začátečníka v pythonu se doporučuje projít tutoriály, které uživatele seznámí se základními příkazy, které se v programu mohou vyskytovat. Program Scapy lze propojit s programem Wireshark. Což umožňuje lepší možnosti pro testování sítě. Je také volně stažitelný a dostupný na webových stránkách programu. Skript wifijammer psaný v jazyce python umí zahlcovat, deautorizovat a zpomalovat WiFi klienty a ostatní přístupové body, které jsou v dosahu. Pro jeho funkčnost je nutné nainstalovat program python, nebo python-scapy. Pro účinnost je zde také vyžadována externí WiFi karta. Tato karta umožní programu wifijammer na jedné síti naslouchat a na druhé ji zahlcovat. Program je velice jednoduchý na instalaci. Není vyžadována zkušenost s jazykem python. Návod, který je k tomuto programu k dispozici na internetu je přehledný a lehce srozumitelný.

Více na.: <https://github.com/DanMcInerney/wifijammer>

Během samotné úlohy jsou k dispozici čtyři routery v rozdílné cenové relaci a úkolem studentů je, tyto routery porovnat z hlediska ovládání a výpadků při měření. Parametry jednotlivých routerů jsou sestaveny pro přehlednost do tabulky.

Název routeru	Standard	Přenosová rychlost [Mbit/s]	Frekvenční rozsah [GHz]
Mercusys MW301R	802.11b,g,n	300	2,4
TP-LINK model TL-WR841N	802.11b,g,n	300	2,4
Netis WF2411	802.11b,g,n	150	2,4
ASUS RT-AC1200G+	802.11a (pro 5GHz), 802.11b,g,n,ac	1167	2,4   5

Tab. 1.5: Parametry routerů

Raspberry Pi jsou malé jednodeskové počítače, které primárně sloužily k ovládání zařízení (pračky, mikrovlnné trouby). Operačním systémem pro Raspberry Pi je Raspbian, ale může na něm fungovat i jiný operační systém. Ve znaku mají tyto minipočítače malinu. Nejlevnější je Raspberry Pi Zero, které umí zachytit vysílání pouze v pásmu 2,4 GHz. Oproti tomu dražší, ale výkonnější Raspberry Pi 4 již dokáže zachytit i pásmo 5 GHz. Raspberry Pi 3 je takový zlatý střed.



Obr. 1.1: Použitá zařízení Raspberry Pi

### **Zadání a postup měření:**

V první části úlohy studenti ověří parametry přenosu dat v síti pro dva, vyučujícím, zvolené routery v čase 10 minut. Vyučující také zvolí, zda bude úloha měřena s RPi 4 a nebo s RPi Zero a zvolí také standard 802.11 b nebo 802.11 n. Pomocí příkazu v teoretické části studenti proměří přenos s protokoly TCP a UDP. U zadaných parametrů budou studenti sledovat zpoždění (delay bit/s) a propustnost (throughput Mbit/s). Z výsledků měření poté sestrojí spojitý grafy (Závislost delay/bitrate), sestrojí přehledné tabulky a zodpoví kontrolní otázky. V druhé části měření studenti zapojí RPi 4 nebo RPi Zero podle toho, se kterým RPi měřili první část. Topologie vypadá následovně:

RPi 3 (iperf3Server), RPi Zero (iperf3Client) a RPi 4 (iperf3Client/wifijammer). S využitím programu Scapy spustí studenti wifijammer na RPi 4, který bude fungovat jako útočník v síti. Studenti proměří tytéž routery a standard 802.11 zvolený v první části měření pro TCP a UDP přenos v čase 10 minut.

Zapojení úlohy je vidět na obrázku níže.



**Obr.1.: Zapojení měřícího pracoviště**

## **Postup**

### **První část měření:**

Vyučující zvolí dva routery, standard a Raspberry Pi ( RPi 4 a nebo RPi Zero), se kterým studenti ověří parametry přenosu v síti. Tyto parametry studenti ověří pro TCP a UDP v čase 10 minut.

#### **1)Nastavení routeru Mercusys**

Router zapojíme do nabíjení. V příkazovém řádku *cmd* zadáme

```
ipconfig
```

a zjistíme požadovanou IP adresu routeru. Ve webovém vyhledávači zadáme požadovanou IP adresu a připojíme se do nastavení routeru. V hlavním okně se objeví vstupní údaje, kde vyplníme přihlašovací jméno a heslo.

*Přihlašovací jméno: student 1234*

*Heslo: student 1234*

Jakmile zadáme požadované přihlašovací údaje, tak vstoupíme do pokročilého nastavení routeru. V záložce Advanced rozklikneme sekci Wireless, zde v poli Mode zvolíme požadovaný standard (802.11b only, 802.11n only), v poli Channel nastavíme volbu

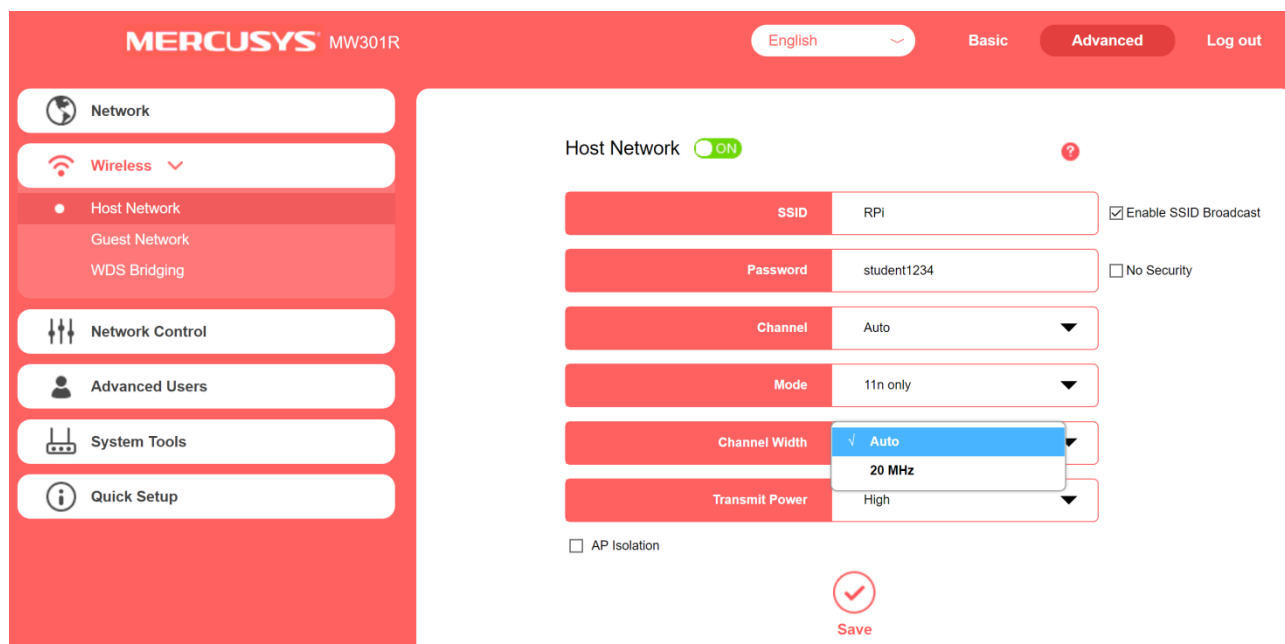
kanálu na automatic, v poli Channel Width zvolíme šířku pásma dle možností požadovaného standardu. Standard 802.11 b podporuje šířku pásma pouze 20 MHz. Pro standard 802.11n budeme volit šířku pásma 20 MHz a 40 MHz. Důležitým posledním krokem je, aby bylo SSID nastaveno na RPi. Až tohle vše zadáme, tak vybranou volbu potvrdíme ve spodní části okna tlačítkem save.

Podrobné nastavení routeru M8ercusys pro standard 802.11 b lze vidět na obrázku níže.

The screenshot displays the web interface of a Mercusys MW301R router. The top navigation bar includes the brand name 'MERCUSYS' and model 'MW301R', a language dropdown set to 'English', and tabs for 'Basic' and 'Advanced' (which is selected). A 'Log out' link is also present. The left sidebar contains a menu with options: 'Network', 'Wireless' (selected), 'Host Network', 'Guest Network', 'WDS Bridging', 'Network Control', 'Advanced Users', 'System Tools', and 'Quick Setup'. The main content area is titled 'Host Network' with a green 'ON' status indicator. It features several configuration fields: 'SSID' set to 'RPi' with a checkbox for 'Enable SSID Broadcast' checked; 'Password' set to 'student1234' with a checkbox for 'No Security' unchecked; 'Channel' set to 'Auto'; 'Mode' set to '11b only'; 'Channel Width' set to '20 MHz'; and 'Transmit Power' set to 'High'. There is also an unchecked checkbox for 'AP Isolation'. At the bottom right, there is a red circular icon with a white checkmark and the text 'Save'.

Obr.1.: Nastavení standardu 802.11 b u routeru Mercusys

Podrobné nastavení routeru Mercusys pro standard 802.11 n lze vidět na obrázku níže.



Obr.1.: Nastavení standardu 802.11 n u routeru Mercusys

Zapojíme úlohu s RPi zero a nebo s RPi 4 dle zadání vyučujícího. Zapojíte RPi do sítě a počkáte, až se načte operační systém u všech RPi. Poté zkontrolujete nastavení v horní liště, zda je RPi připojeno pouze k síti RPi. Abychom zjistili IP adresu klienta, nebo serveru je nutné zadat do příkazového řádku *cmd*

```
ifconfig
```

Spojení pak lze ověřit pomocí příkazu

```
Ping 192.168.x.x
```

na IP adresu klienta nebo serveru. Pokud vše funfuje, tak do příkazového v již spuštěném RPi řádku vypíšeme následující:

Na iperf3Server zadáme do příkazového řádku:

```
iperf3 -s
```

Tento příkaz umožní serveru naslouchat na portu 5060. A umožní mu komunikovat s klientem.

Na Iperf3Client spustíme dva příkazové řádky, kde na jednom napíšeme příkaz pro testování propustnosti sítě a na druhém příkaz na zjištění zpoždění.

V prvním příkazovém řádku napíšeme

```
iperf3 -c 192.168.x.x -u -t 600 -b 20m >> D:\\název souboru.xls
```

Parametr *-t* je čas trvání testu

Čas volíme na 10 minut = 600 s

Parametr *-b* je maximální rychlost generování dat souvisí se standardem, který v měření bude použit a na také na možnostech routeru. Pro standard 802.11 b je použit parametr

*-b 20 m* (Maximální přenosová rychlost standardu 802.11b 11 Mbit/s). Pro standard 802.11 n se použije parametr *-b 350m*.

Parametr *-u* značí, že se jedná o testování protokolu UDP. Pokud cheme testovat TCP přenos, tak místo mezi IP adresou a parametrem *-t* zůstane volné.

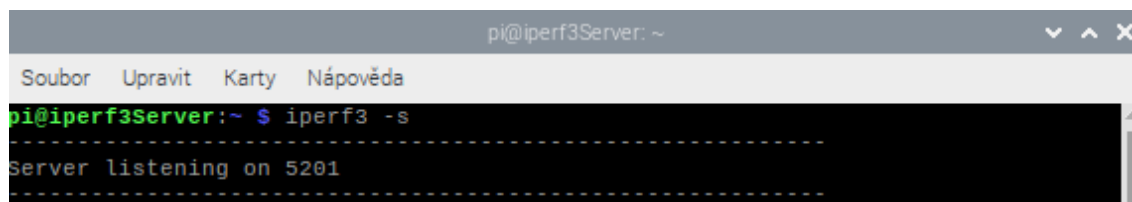
V druhém příkazovém řádku napíšeme příkaz

```
ping 192.168.x.x -c 605 >> D:\\název souboru.xls
```

Parametr *-c* značí, jak dlouho má ping probíhat

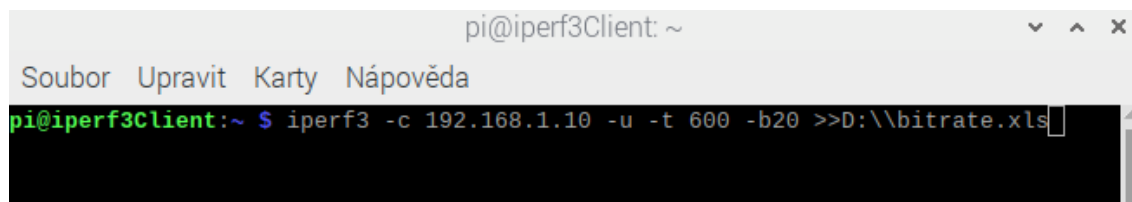
Pokud máme vše vypsáno, tak před zahájením testování zkontrolujeme, zda je RPi připojeno k RPi. Pokud je vše v pořádku, nejprve potvrdíme příkaz u RPi 3 Server a teprve až potom spustíme zároveň příkazy sepsané na RPi Zero Client.

Celé nastavení parametrů s využitím programu Iperf3 je zobrazeno níže:



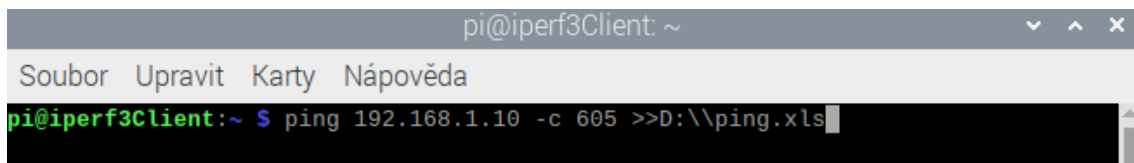
```
pi@iperf3Server: ~  
Soubor Upravit Karty Nápověda  
pi@iperf3Server:~ $ iperf3 -s  
-----  
Server listening on 5201  
-----
```

Obr. 1.9: Příkaz na RPi 3 (iperf3Server)



```
pi@iperf3Client: ~  
Soubor Upravit Karty Nápověda  
pi@iperf3Client:~ $ iperf3 -c 192.168.1.10 -u -t 600 -b20 >>D:\\bitrate.xls
```

Obr.1.10: Příkaz na ověření propustnosti



Obr.1.11: Příkaz na ověření zpoždění

Po spuštění vyčkáme 10 minut uložení hodnot do dvou souborů. Jakmile testování skončilo, v již otevřené aplikaci Bitvise zadáme:

Host: IP dresa RPi Zero (iperf3Client)

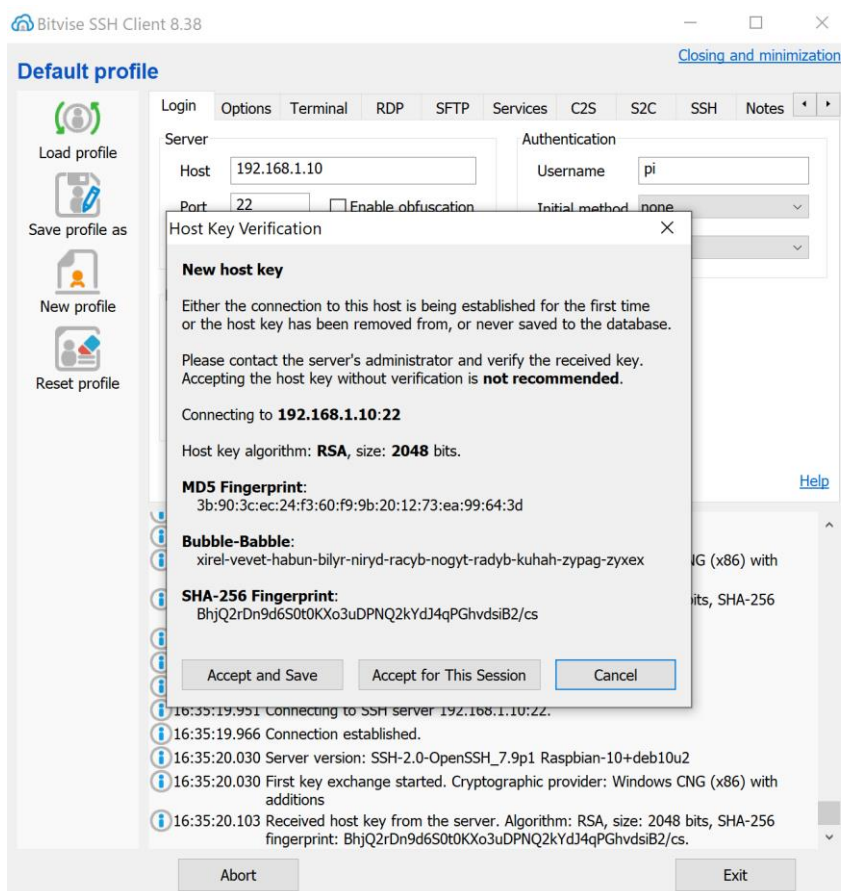
Port: 22

Username: pi

dále klikneme na Log in. Poté zaškrtneme Accept for This Session a objeví se okno, kde zadáme heslo.

heslo: raspberry

Poté je postup stejný jako při používání Total Commander.



Obr.1.12: Postup při zpracování dat v aplikaci Bitvise

## 2) Nastavení routeru Netis

Router zapojíme do nabíjení. V příkazovém řádku *cmd* zadáme

```
ipconfig
```

a zjistíme požadovanou IP adresu routeru. Ve webovém vyhledávači zadáme požadovanou IP adresu a připojíme se do nastavení routeru. V hlavním okně se objeví vstupní údaje, kde vyplníme přihlašovací jméno a heslo.

Přihlašovací jméno: student 1234

Heslo: student 1234

Jakmile zadáme požadované přihlašovací údaje, tak vstoupíme do pokročilého nastavení routeru. V záložce Advanced rozklikneme sekci Wireless, zde v poli Mode zvolíme požadovaný standard (802.11b only, 802.11n only), v poli Channel nastavíme volbu kanálu na automatic, v poli Channel Width zvolíme šířku pásma dle možností požadovaného standardu. Standard 802.11 b podporuje šířku pásma pouze 20 MHz. Pro standard 802.11n budeme volit šířku pásma 20 MHz a 40 MHz. Důležitým posledním krokem je, aby bylo SSID nastaveno na RPi. Až tohle vše zadáme, tak vybranou volbu potvrdíme ve spodní části okna tlačítkem save.



Podrobné nastavení routeru Netis se standardem 802.11 b lze vidět na obrázku níže.

**netis**

**WF2411**

- Stav
- Síť
- WiFi 2.4G
  - Nastavení WiFi
  - Filtrování adres MAC
  - Nastavení WPS
  - Více SSID
  - Rozšířené WiFi
  - Seznam klientů
- Nastavení QoS
- Forwarding
- Filtrování přístupu
- Dynamická DNS
- Upřesnit
- Systémové nástroje
- Select Language

### Nastavení WiFi připojení

Stav : ☒ Zapnout ☐ Vypnout

MAC adresa : 04:8d:38:4f:06:39

Režim rádia : Přístupový bod

Rádiové pásmo : 802.11b

SSID : RPi

Vysílání SSID : ☒ Zapnout ☐ Vypnout

Region : EU

Kanál : Automaticky

### Nastavení zabezpečení AP

Pro zajištění optimálního zabezpečení vaší WiFi sítě důrazně doporučujeme nastavit typ ověřování WPA2-PSK a typ šifrování AES nebo TKIP a AES.

Typ ověřování : WPA/WPA2-PSK

Typ šifrování : ☒ TKIP a AES

Režim klíče : ☐ HEX ☒ ASCII

Heslo : student1234 (Zadejte 8 - 63 znaků ASCII (a-z, A-Z, 0-9.))

Obr.1.: Nastavení standardu 802.11 b u routeru Netis

Podobné nastavení routeru Netis se standardem 802.11 n lze vidět na obrázku níže.

**netis**

**WF2411**

- Stav
- Síť
- WiFi 2.4G
  - Nastavení WiFi
  - Filtrování adres MAC
  - Nastavení WPS
  - Více SSID
  - Rozšířené WiFi
  - Seznam klientů
- Nastavení QoS
- Forwarding
- Filtrování přístupu
- Dynamická DNS
- Upřesnit
- Systémové nástroje
- Select Language

### Nastavení WiFi připojení

Stav : ☒ Zapnout ☐ Vypnout

MAC adresa : 04:8d:38:4f:06:39

Režim rádia : Přístupový bod

Rádiové pásmo : 802.11n

SSID : RPi

Vysílání SSID : ☒ Zapnout ☐ Vypnout

Region : EU

Kanál : Automaticky

Šířka kanálu : ☐ 20 MHz ☒ 40 MHz ☐ 20/40MHz

Řízení Postranní pásmo : ☐ Dolní ☒ Horní

### Nastavení zabezpečení AP

Pro zajištění optimálního zabezpečení vaší WiFi sítě důrazně doporučujeme nastavit typ ověřování WPA2-PSK a typ šifrování AES nebo TKIP a AES.

Typ ověřování : WPA/WPA2-PSK

Typ šifrování : ☒ TKIP a AES

Režim klíče : ☐ HEX ☒ ASCII

Heslo : student1234 (Zadejte 8 - 63 znaků ASCII (a-z, A-Z, 0-9.))

Obr.1.: Nastavení standardu 802.11 n u routeru Netis

Pro měření routeru Netis jsou všechny příkazy stejné jako v případě nastavení routeru Mercusys. Mění se pouze parametr *-b* pro standard 802.11 n. Zde se zvolil parametr *-b 200 m*. Tento parametr se měnil kvůli maximální přenosové rychlosti standardu 802.11n, která je oproti ostatním routerům pouze 150 Mbit/s.

### 3) Nastavení routeru TP-Link

Router zapojíme do nabíjení. V příkazovém řádku *cmd* zadáme

```
ipconfig
```

a zjistíme požadovanou IP adresu routeru. Ve webovém vyhledávači zadáme požadovanou IP adresu a připojíme se do nastavení routeru. V hlavním okně se objeví vstupní údaje, kde vyplníme přihlašovací jméno a heslo.

Přihlašovací jméno: student 1234

Heslo: student 1234

Jakmile zadáme požadované přihlašovací údaje, tak vstoupíme do pokročilého nastavení routeru. V záložce Advanced rozklikneme sekci Wireless, zde v poli Mode zvolíme požadovaný standard (802.11b only, 802.11n only), v poli Channel nastavíme volbu kanálu na automatic, v poli Channel Width zvolíme šířku pásma dle možností požadovaného standardu. Standard 802.11 b podporuje šířku pásma pouze 20 MHz. Pro standard 802.11n budeme volit šířku pásma 20 MHz a 40 MHz. Důležitým posledním krokem je, aby bylo SSID nastaveno na RPi. Až tohle vše zadáme, tak vybranou volbu potvrdíme ve spodní části okna tlačítkem Save.

Podrobné nastavení routeru Tp-Link standardu 802.11b lze vidět na obrázku níže.

**TP-LINK®**

**Wireless Settings**

Wireless Network Name:  (Also called the SSID)

Region:

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode:

Channel Width:

Channel:

Please use the WiFi switch on this device to enable/disable radio

☒ Enable Wireless Router Radio

☒ Enable SSID Broadcast

☐ Enable WDS Bridging

Obr.1.: Nastavení standardu 802.11 b u routeru TP-Link

Podrobné nastavení routeru Tp-Link standardu 802.11n lze vidět na obrázku níže.

**TP-LINK®**

**Wireless Settings**

**Wireless Network Name:** RPi (Also called the SSID)

**Region:** Czech Republic

**Warning:** Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

**Mode:** 11n only

**Channel Width:** Auto

**Channel:** Auto

Please use the WiFi switch on this device to enable/disable radio

☒ Enable Wireless Router Radio

☒ Enable SSID Broadcast

☐ Enable WDS Bridging

Save

Obr.1.: Nastavení standardu 802.11 n u routeru TP-Link

U nastavení 802.11 n se měnila pouze hodnota Channel Width. Tato hodnota se nastavovala na auto, 20 MHz a 40 MHz.

Pro měření routeru Tp-Link jsou všechny příkazy stejné jako v případě nastavení routeru Mercusys.

#### 4) Nastavení routeru Asus

Router zapojíme do nabíjení. V příkazovém řádku *cmd* zadáme

```
ipconfig
```

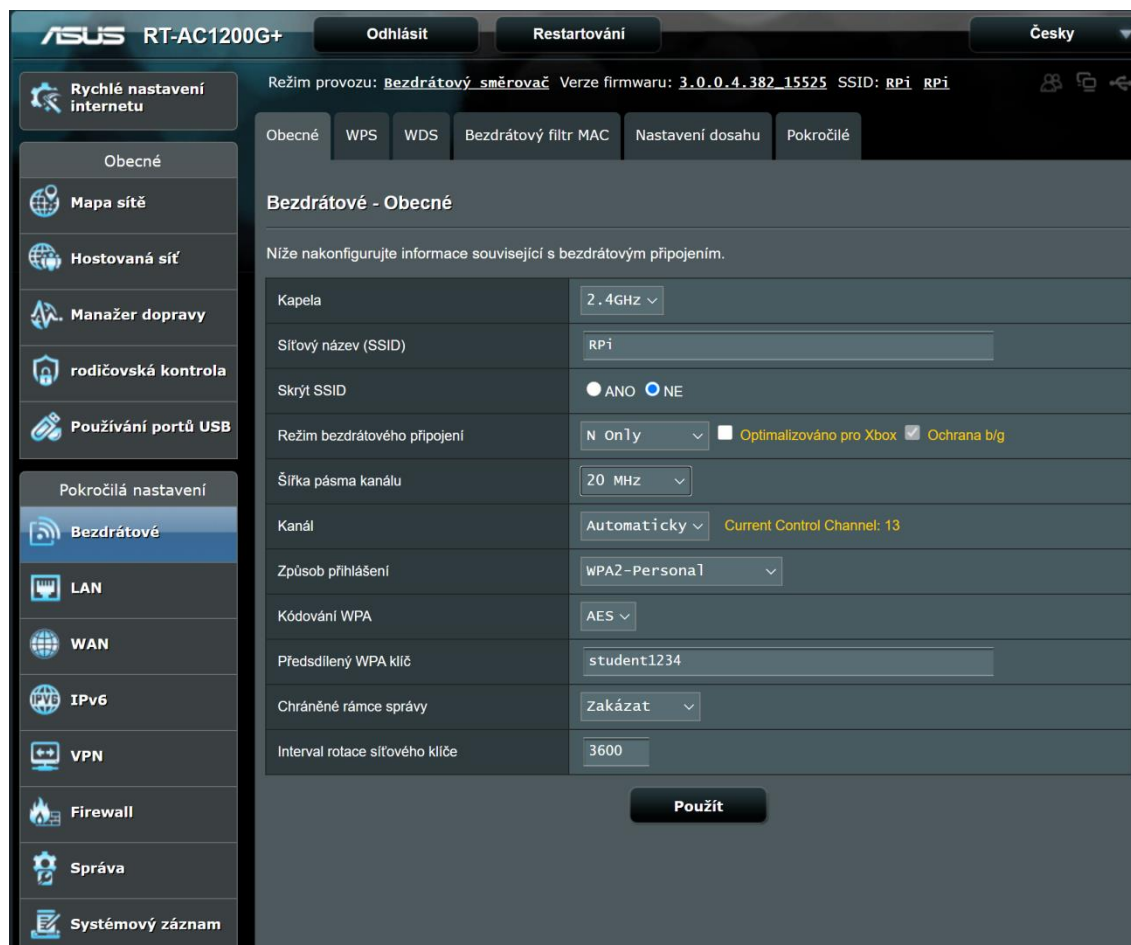
a zjistíme požadovanou IP adresu routeru. Ve webovém vyhledávači zadáme požadovanou IP adresu a připojíme se do nastavení routeru. V hlavním okně se objeví vstupní údaje, kde vyplníme přihlašovací jméno a heslo.

Přihlašovací jméno: student 1234

Heslo: student 1234

Jakmile zadáme požadované přihlašovací údaje, tak vstoupíme do pokročilého nastavení routeru. V záložce Advanced rozklikneme sekci Wireless, zde v poli Mode zvolíme požadovaný standard (802.11b only, 802.11n only), v poli Channel nastavíme volbu kanálu na automatic, v poli Channel Width zvolíme šířku pásma dle možností požadovaného standardu. Standard 802.11 b podporuje šířku pásma pouze 20 MHz. Pro standard 802.11n budeme volit šířku pásma 20 MHz a 40 MHz. Důležitým posledním krokem je, aby bylo SSID nastaveno na RPi. Až tohle vše zadáme, tak vybranou volbu potvrdíme ve spodní části okna tlačítkem save.

Podrobné nastavení routeru Asus standardu 802.11 n lze vidět na obrázku níže.



Obr.1.: Nastavení standardu 802.11 n u routeru Asus

Pro měření routeru Asus jsou všechny příkazy stejné jako v případě nastavení routeru Mercusys. Mění se pouze nastavení šířky pásma kanálu na hodnotu 20 MHz a 40 MHz.

## 2 část měření:

V programu Python nainstalovaném na RPi 4 (iperf3Client/wifijammer) spustí studenti wifijammer, který bude fungovat jako útočník na síť. Pro dva, vyučujícím, zvolené routery a standard studenti proměří rušení dle následující topologie: RPi 3 (iperf3Server), RPi 4(iperf3Client/wifijammer) a RPi Zero (iperf3Client). Testování bude pro zvolené routery a standard z předchozího bodu měření a v čase 10 minut. Test bude proveden pro TCP a UDP přenos.

Nastavení jednotlivých routerů je stejné jako v první části měření

1) Mercusys

2) Netis

3) TP-Link

4) Asus

V druhé části úlohy se k RPi 3 (iperf3Server) a RPi Zero (iperf3Client) přidal RPi 4 v roli (iperf3Client/wifijammer). Ten má pomocí skriptu wifijammer zahltit přenos v síti. RPi 4 (iperf3Client/wifijammer) budete ovládat pomocí vzdáleného přístupu. Během testování je nutné zkontrolovat, zda je zařízení připojeno k síti RPi.

V příkazovém řádku zadáte příkaz

```
ls
```

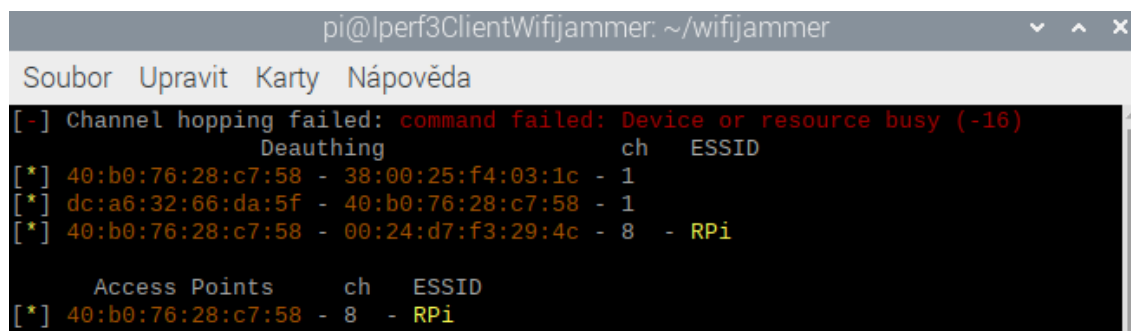
který ukáže, zda je ve složce soubor wifijammer.py. Po přepnutí do složky, která obsahuje soubor wifijammer.py, se dostanete pomocí příkazu

```
cd wifijammer/
```

Aby bylo možné program ovládat, je nutné být v režimu superuživatele. To provedete příkazem

```
sudo python wifijammer.py
```

Pak tento příkaz potvrdíte tlačítkem enter. Program se poté spustí ale zároveň deautorizuje všechny sítě v okolí. Také však zobrazí použitou MAC adresu RPi, kterou si zaznamenejte. Viz obrázek níže:



```
pi@lperf3ClientWifijammer: ~/wifijammer
Soubor Upravit Karty Nápověda
[-] Channel hopping failed: command failed: Device or resource busy (-16)
      Deauthing          ch  ESSID
[*] 40:b0:76:28:c7:58 - 38:00:25:f4:03:1c - 1
[*] dc:a6:32:66:da:5f - 40:b0:76:28:c7:58 - 1
[*] 40:b0:76:28:c7:58 - 00:24:d7:f3:29:4c - 8 - RPi
      Access Points      ch  ESSID
[*] 40:b0:76:28:c7:58 - 8 - RPi
```

Obr.1.21: Zobrazení MAC adresy zařízení RPi

Poté už jen zadáte testovací parametry. Celý příkaz na testování:

```
Sudo python wifijammer.py -a x:x.x:x:x -c x -d -i wlan0 -p x -t x
```

kde:

-a značí použitou MAC adresu RPi

-c označuje kanál, na kterém dané RPi vysílá. Tento kanál je pro všechna RPi zvolen stejně. A je možné jej zjistit vedle zobrazené MAC adresy.

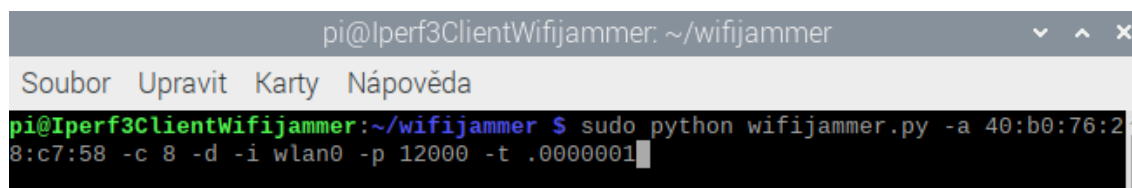
-d značí, že se nebude deautorizovat síť v průběhu vysílání

-i značí použité rozhraní

-p označuje počet paketů, které byly během testování odeslány. Pro standard 802.11 b nastavíte hodnotu odeslaných paketů na 1200. Při větší hodnotě by docházelo k výpadku celé komunikace. Pro standard 802.11 n tuto hodnota nastavíte na 25000. Při větší hodnotě už by opět docházelo k výpadkům komunikace.

-t označuje čas, za který se tyto pakety opakovaně přenášely. Pro testování nastavíte hodnotu 0.00000001 s.

Blíže je tento příkaz vidět na obrázku níže.

A screenshot of a terminal window titled 'pi@lperf3ClientWifijammer: ~/wifijammer'. The window has a menu bar with 'Soubor', 'Upravit', 'Karty', and 'Nápověda'. The terminal shows a command prompt 'pi@Iperf3ClientWifijammer:~/wifijammer \$' followed by the command 'sudo python wifijammer.py -a 40:b0:76:28:c7:58 -c 8 -d -i wlan0 -p 12000 -t .00000001'. The command is partially highlighted in green and blue.

Obr.1.22:Příkaz pro zahlcení standardu 802.11 b

Během testování jaminngu nejprve spustíte příkazem server, poté program wifijammer a nakonec klienta, na kterém byly paralelně nastaveny příkazy na testování propustnosti a zpoždění při přenosu.

Po testování, které bude trvat 10 minut, uložené hodnoty zpracujete do přehledných spojitých grafů.



**Kontrolní otázky:**

- 1) Jaký je rozdíl mezi TCP a UDP protokolem?
- 2) Které pásmo má lepší dosah přes překážky a které pásmo se méně zahlcuje?
- 3) Jaké jsou maximální přenosové rychlosti u zvoleného standardu 802.11b/802.11n daného routeru?
- 4) Co to je jamming a jak funguje?
- 5) Na které vrstvě TCP/IP pracují protokoly TCP a UDP?

**Odpovědi na kontrolní otázky:**

1) TCP (Transmission Control Protocol) zajišťuje spolehlivý přenos dat v síti, zaručuje bezztrátový přenos

UDP(User Datagram Protocol) zajišťuje nespolehlivý přenos dat v síti

2) Nejlepší dosah přes překážky má pásmo 2,4 GHz. Menší zahlcení provozu je však u pásma 5 GHz.

3) Pro router Mercusys: Standard 802.11 b má maximální přenosovou rychlost 11Mbit/s. Standard 802.11 n má maximální přenosovou rychlost 300 Mbit/s.

Pro router Netis: Standard 802.11 b má maximální přenosovou rychlost 11Mbit/s. Standard 802.11 n má maximální přenosovou rychlost 150 Mbit/s.

Pro router Tp-Link: Standard 802.11 b má maximální přenosovou rychlost 11Mbit/s. Standard 802.11 n má maximální přenosovou rychlost 300 Mbit/s.

Pro router Asus: Standard 802.11 b má maximální přenosovou rychlost 11Mbit/s. Standard 802.11 n má maximální přenosovou rychlost 300 Mbit/s.

4) jamming je program, který má funkci útočníka v síti

Při zadání příkazu, který spustí jamming, má tento program výrazně snížit přenosovou rychlost, zvětšit zpoždění a větší ztrátovost paketů.

5) Protokoly TCP a UDP pracují na transportní vrstvě modelu TCP/IP

**Použité přístroje:**

RPi 3, RPi Zero, RPi 4, dva monitory, dvě klávesnice a myši, napájecí kabely na všechna zařízení, propojovací kabely


**Závěr:**

Do závěru student zhodnotí body měření podle postupu v zadání. Okomentuje vzniklé grafické průběhy a hodnoty zaznamená do přehledných tabulek. Také zhodnotí, zda se výsledky shodují s teoretickými předpoklady a může také zmínit problémy, které se objevily během měření.

**Použitá literatura:**

- [1] JEŘÁBEK, J. Komunikační technologie. Brno: Vysoké učení technické v Brně, 2019. s. 1-175. ISBN: 978-80-214-4713-4. (cs)
- [2] BVKS, Laboratorní cvičení. Komunikační technologie Wi-Fi. FEKT, Brno 2018. s. 1-20. (cs)
- [3] BARS, Laboratorní cvičení. Komunikace v sítích WLAN. FEKT, Brno 2018. s. 1-7. (cs)

## Příloha 4 - Vzorový protokol

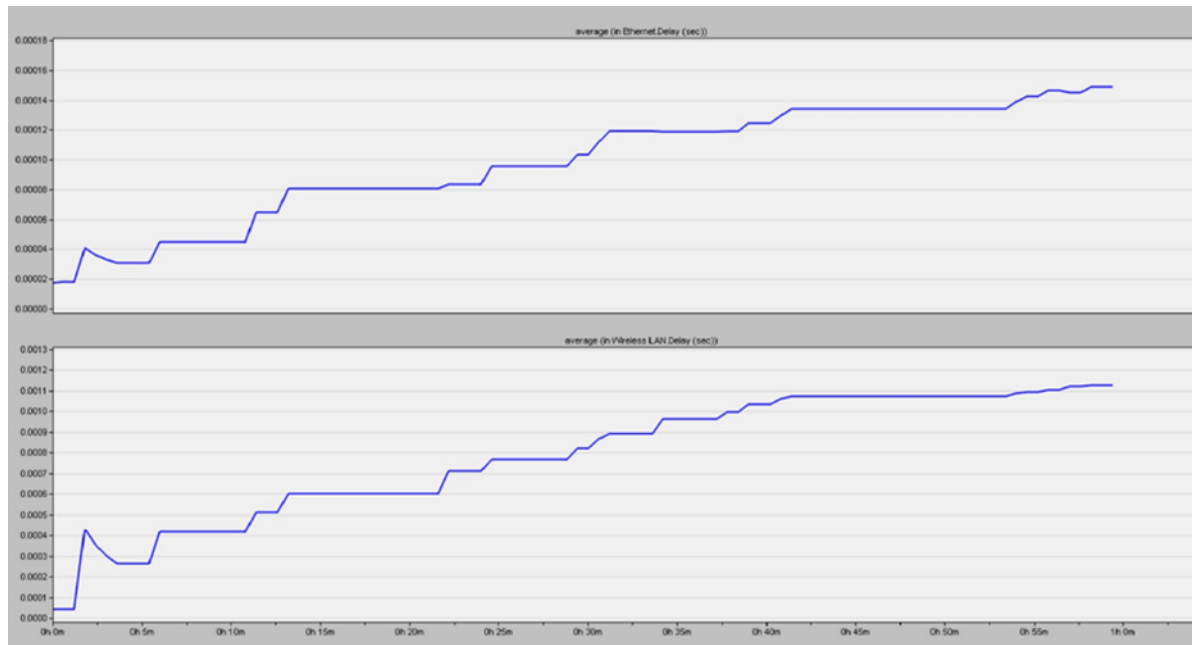
		Předmět <b>Přístupové a transportní sítě</b>	
		Jméno	
		Ročník	
		Spolupracoval	Měřeno dne
Kontroloval		Hodnocení	
Číslo úlohy	Název úlohy  <b>Vzájemné testování WLAN sítí v pásmu 2,4 GHz</b>		

### Zadání:

- 1) V prvním bodě zadání jsme sestavili zapojení laboratorní úlohy dle schématu v zadání. Důležité bylo vybrat správné komponenty z palety Object Palette Tree a tyto komponenty propojit linkou 100BaseT.
- 2) Ve druhé části zadání jsme konfigurovali jednotlivé routery použité v sestavení laboratorní úlohy. Nejdůležitější bylo nastavení parametru BSS Identifier u jednotlivých routerů.
- 3) Ve třetí části zadání jsme nastavovali pracovní stanice tak, aby parametr BSS Identifier byl nastaven podle nastavení routerů. A tedy WLAN\_Use1 měl nastavenou hodnotu BSS Identifier na hodnotu 1, tak aby odpovídal nastavení BSS Identifier pro WLAN\_Router1.
- 4) Ve čtvrté části zadání úlohy bylo nejdůležitější v liště Protocols => Wireless LAN => Configure PHY and Data Rate, nastavit požadovaný standard a přenosovou rychlost podle zadání.
- 5) V páté části zadání jsme nakonfigurovali komponenty Application Config a Profile Config. Zde bylo zásadní správně nastavit u Profile Config parametr Supported Profiles.
- 6) V šestém bodě jsme měli nastavit server a jeho parametr Supported Services.
- 7) V sedmém bodě zadání jsme měli nastavit a zobrazit sledované statistiky z měření. Bylo nutné správně zvolit nastavení sledovaných statistik v záložce Global Statistics. Tyto statistiky se nám zobrazili po kliknutí na horní lištu, kde se zvolilo View Results.

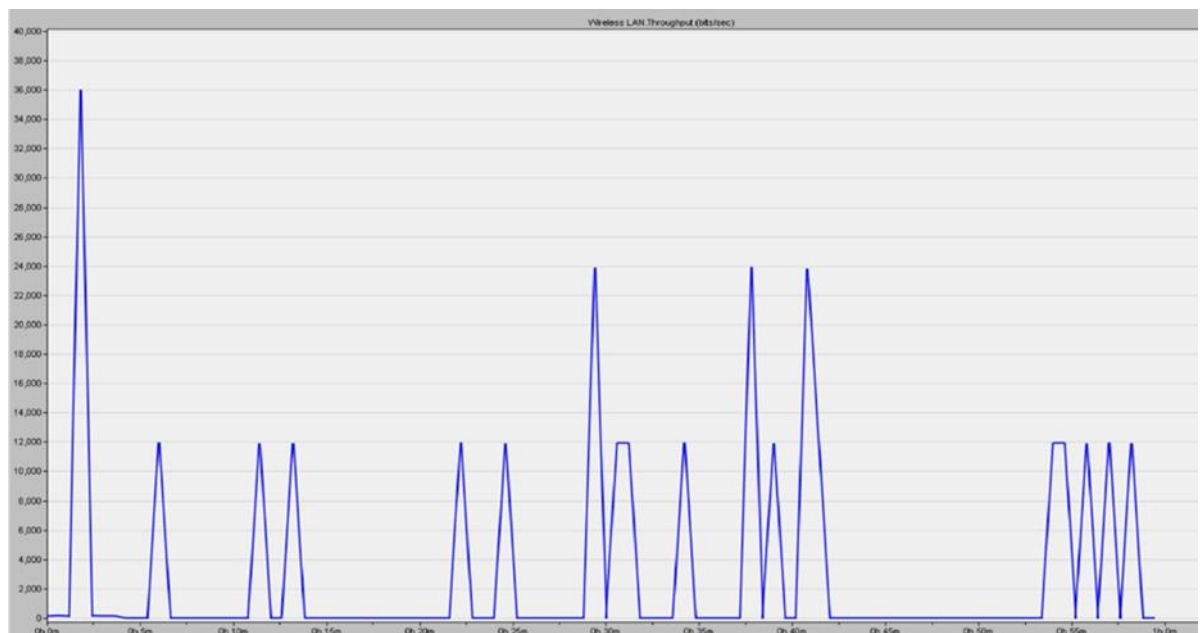
## Grafy:

Graf sledované statistiky Delay:

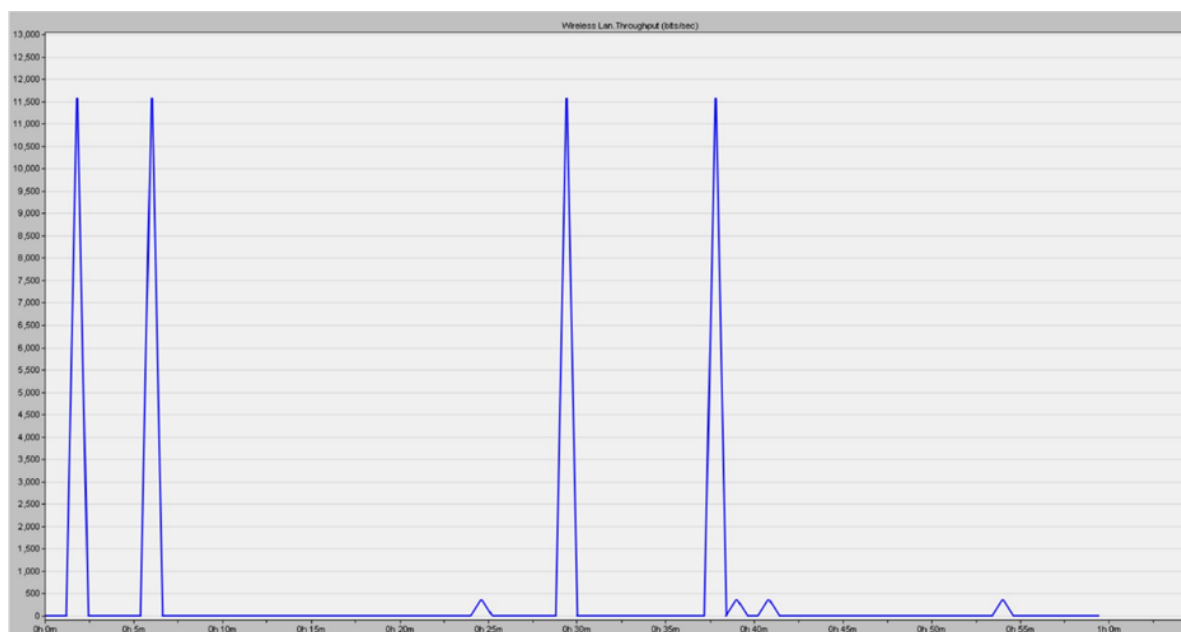


Obr.1.8: Zpoždění

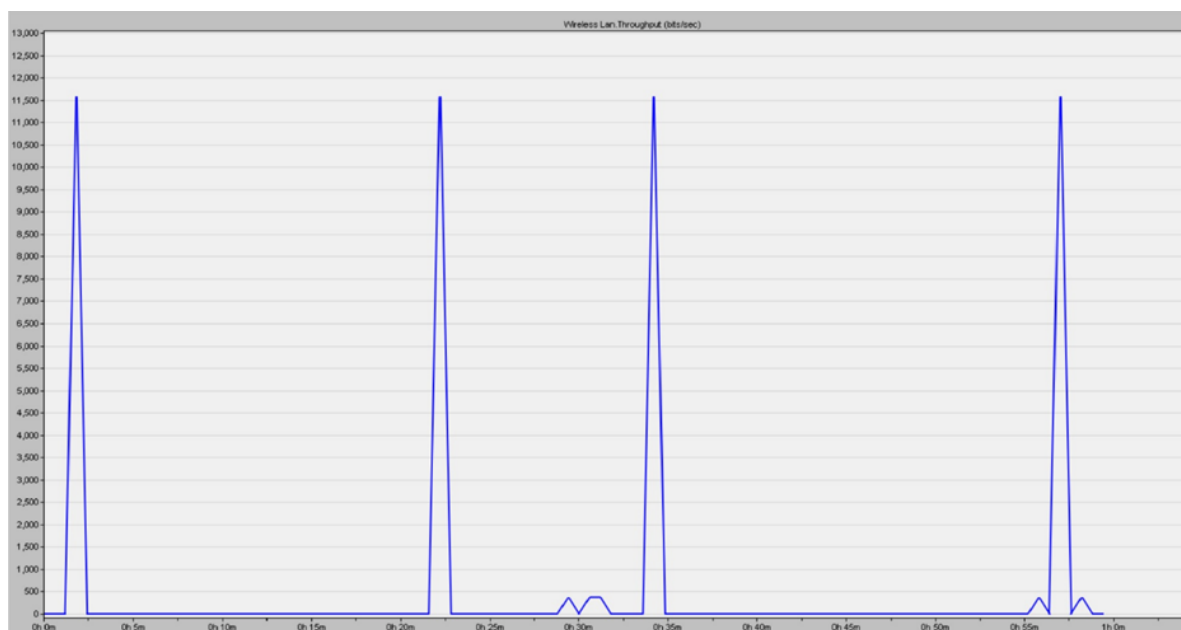
Graf sledované statistiky Throughput:



Obr.1.4: Celková propustnost



Obr.1.5: Propustnost routeru 1



Obr.1.6: Propustnost routeru 2




Obr.1.7: Propustnost routeru 3

### **Závěr:**

V laboratorní úloze Vzájemné testování WLAN sítí v pásmu 2,4 GHz jsme se v první části zadání měli seznámit s obsluhou programu Riverbed Modeler, ve kterém jsme měli za úkol sestavit síť složenou ze tří routerů, serveru, switchu a třech pracovních stanic podle topologie v návodu. V druhé části laboratorní úlohy jsme měli za úkol nakonfigurovat jednotlivé routery podle zadání. Ve třetí části úlohy jsme měli za úkol nastavit pracovní stanice a jejich hodnotu BSS Identifier, kterou jsme nastavovali v rozmezí 1-3. Ve čtvrté části úlohy jsme měli za úkol nastavit standard vhodný pro toto testování a tedy standard 802.11g a přenosovou rychlost 54 Mbit/s. V páté a šesté části úlohy jsme nakonfigurovali komponenty Application Config a Profile Config, kde jsme měli správně nastavit u Profile Config parametr Supported Profiles a u Application Config parametr Supported Services. V sedmém bodě úlohy jsme měli nastavit a zobrazit sledované statistiky z měření. U grafu zpoždění je opatrné, že během časového úseku, který trval 1 hodinu, tak docházelo k postupnému nárůstu zpoždění. Na x-ové ose je vidět čas simulace v programu Riverbed v minutách a na x-ové ose je zpoždění v sekundách. V čase 2,5 minuty došlo k nárůstu zpoždění z nuly na více jak 4 sekundy. To je způsobeno tím, že bylo nastaveno File Transfer Heavy při konfiguraci Application Config a Profile Config. Standard 802.11g využívá pásmo 2,4 GHz a přenosovou rychlost 54 Mbit/s. Realná přenosová rychlost během přenosu však byla mnohem menší. To způsobilo

kolísání zpoždění, kdy v časech 2,5 minuty, 12 minut, 22 minut, 32 minut, 42 minut docházelo k výkyvům zpoždění. Zpoždění se ustálilo až po 42 minutách měření. U grafu propustnosti routeru 1 je vidět, že je tento router podobně jako router 3 ovlivněn buď topologií sítě (odchýlení, vzdálenost) a nebo jeho nastavením (kanál), kdy nebylo možné nastavit jeden kanál ale tento kanál se vybíral náhodně. To mohlo způsobit ovlivnění propustnosti všech těchto routerů. Z grafu je také patrné, že tento router zachytával a propouštěl nejvíce dat ve 2 minutách, 6 minutách, 28 minutách a 38 minutách. Ke konci simulace tento router již nevykazoval téměř žádnou aktivitu. U grafu propustnosti routeru 2 je vidět, že měl tento router během hodinové simulace nejstabilnější propustnost. Tento router data aktualizoval nejenom na začátku simulace, ale i v průběhu a na konci simulace. To může být způsobeno jeho umístěním do pomyslné přímky v topologii sítě. Tyto výsledky mohly být také ovlivněny nastavením routeru, kdy v programu nešel přímo nastavit kanál, ale tento kanál se nastavoval automaticky pro každý router. I to mohlo způsobit kolísání a propustnost dat jen v určitý okamžik simulace. U grafu propustnosti routeru 3 je vidět, že měl tento router během hodinové simulace největší okamžik propustnosti ve 2 minutách a ve 48 minutách. Z grafu je také patrné, že samotná propustnost dat u routeru 3 ukazuje mnohem více nulových dat než u routeru 1 a routeru 2. Tato nulová data mohou být způsobena topologií sítě (router 3 byl odchýlen, moc vzdálen), mohla být také způsobena nastavením routeru (kanál). Z grafu celkové propustnosti je vidět, že byl ale přenos a propustnost dat v průběhu celé simulace. Což bohužel ale vypovídá tomu, že když chtěl data posílat jeden router, tak druhý ho neblokoval. Vypovídá to však také o tom, že celková propustnost v síti je zhruba poloviční, oproti propustnosti jednotlivých routerů, ale dostačující. Není zde vidět moc dat, které se vůbec nepřenesly.

## Příloha 5 - Vzorový protokol č.2

		Předmět <b>Přístupové a transportní sítě</b>	
		Jméno	
		Ročník	
		Spolupracoval	Měřeno dne
Kontroloval		Hodnocení	
Číslo úlohy	Název úlohy  <b>Vzájemné rušení WLAN sítí</b>		

### Zadání:

V první části úlohy studenti ověří parametry přenosu dat v síti pro dva, vyučujícím, zvolené routery v čase 10 minut. Vyučující také zvolí, zda bude úloha měřena s RPi 4 a nebo s RPi Zero a zvolí také standard 802.11 b nebo 802.11 n. Pomocí příkazu v teoretické části studenti proměří přenos s protokoly TCP a UDP. U zadaných parametrů budou studenti sledovat zpoždění (delay bit/s) a propustnost (throughput Mbit/s). Z výsledků měření poté sestojí spojitě grafy (Závislost delay/bitrate), sestojí přehledné tabulky a zodpoví kontrolní otázky. V druhé části měření studenti zapojí RPi 4 nebo RPi Zero podle toho, se kterým RPi měřili první část. Topologie vypadá následovně: RPi 3(server), RPi Zero (Client) a RPi 4 (Client/wifijammer). S využitím programu Scapy spustí studenti WiFi jammer na RPi 4, který bude fungovat jako útočník v síti. Studenti proměří tytéž routery a standard 802.11 zvolený v první části měření pro TCP a UDP přenos v čase 10 minut.

**Grafy a tabulky** s naměřenými hodnotami pro první i druhou část se nacházejí v příloze kvůli velkému počtu hodnot.



**Závěr:**

Každý student do závěru zhodnotí, pro který standard a šířku pásma, byla nejnižší přenosová rychlost, nejvyšší zpoždění a největší ztrátovost při použití skriptu wifijammer. Také do závěru zhodnotí, který ze dvou routerů vykazuje nejvyšší přenosovou rychlost, nejmenší zpoždění a také nejmenší ztrátovost. Vytvoří spojitě grafy závislosti přenosové rychlosti (bitrate) na zpoždění (delay) z hodnot první části měření a také vytvoří spojitý graf závislosti přenosové rychlosti (bitrate) na zpoždění (delay) při použití skriptu wifijammer. Pro velké množství dat a grafů jsou všechny tyto hodnoty naměřeny a vloženy do příloh. Do závěru také student zhodnotí měření z hlediska náročnosti a uvede, který router bylo pro něj snazší nastavit. Vzhledem k tomu, že tato laboratorní úloha byla měřena v domácích podmínkách, mohou ty laboratorní vykazovat jiné hodnoty.

## Příloha 5a - Popis routeru Mercusys MW301R

V této části je popsán použitý hardware při vypracování laboratorní úlohy. Tento hardware poslouží při vypracování úlohy jako pomůcka, podle které se budou volit jednotlivé prvky v programu Riverbed, aby co nejvíce odpovídali reálným routerům použitým v laboratorní úloze v bakalářské práci.

Na realizaci rušení v laboratorní úloze je vhodné vybrat WLAN router, který bude mít nejnižší frekvenční pásmo a nejnižší přenosovou rychlost. Jelikož je nutné síť zahltit, pak je nutné těchto WLAN routerů sehnat co možná nejvíc. Pro realizaci laboratorní úlohy by měly postačit 3 tyto routery. Vzhledem k předchozím parametrům na nižší frekvenční pásmo a přenosovou rychlost je vhodný router WLAN 2,4 GHz Mercusys včetně napájení. Samotný Mercusys disponuje těmito parametry: Možnost většího pokrytí pomocí dvou výkonných antén, jejichž zisk je 5dBi. Antény vylepšují příjem signálu a jeho citlivost a díky tomu je tento router schopný širokého bezdrátového pokrytí. Využívá přenosovou rychlost 300Mb/s, která je vhodná na HD streaming, online hraní her a rychlé stahování souborů. Nabízí také velmi jednoduchou instalaci, která se skládá ze třech kroků. Při nastavení není nutná žádná složitá konfigurace. Na webových stránkách lze podle návodu postupovat krok po kroku a samotné zprovoznění routeru je hotové během něho lika minut.

Obecné parametry na routeru Mercusys:

Model:MW301R

Typ: WiFi Router

Podporované standardy: 802.11b, 802.11g, 802.11n

Typ a počet antén: 2 fixní antény

Síla antény: 2 x 5dBi

Počet portů RJ-45 a HUBu/Switchu: 3/2

Přenosová rychlost WLAN: 300 [Mb/s]

Rozhraní: RJ-45, WiFi

Frekvenční rozsah: 2,4 [GHz]

Výrobce: TP-Link Czech s.r.o [39]



Obrázek 1 Router Mercusys MW301R [43]

## Příloha 5b – Popis routeru TP - LINK model TL-WR841N

Docílení rušení však nemusí být pouze WLAN routery se stejným frekvenčním pásmem, ale i s rozdílnými frekvenčními pásmy. Proto je vhodné zvolit routery, které budou mít i určité parametry odlišné. Dalším routerem použitým při realizaci laboratorní úlohy je router TP-Link, který je vhodný pro použití v domácnostech, ale i v malých podnicích. Tento router disponuje větší bezpečností bezdrátového ale i kabelového připojení. Technologie 2T2R MIMO si poradí se streamováním, voláním přes VoIP a nebo s hraním online her. Přenos dat je rychlejší díky přenosové rychlosti 300 Mbit/s. Výrobce garantuje, díky technologii CCA (Clear Channel Assessment), stabilní a maximálně rychlý přenos.

Obecné parametry routeru TP-Link jsou:

Model: TL-WR841N

Typ: WiFi Router

Podporované standardy: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

Typ a počet antén: Pevná Omni Directional Antenna X 2

Síla antény: 2 x 5 dBi

Přenosová rychlost WLAN: 300 Mb/s, v případě standardu IEEE 802.11b je přenosová rychlost pouze 11Mb/s.

Rozhraní: RJ45, WiFi

Frekvenční rozsah: 2,4 - 2,4835 GHz

Výrobce: TP-Link Czech s.r.o [38]

Router TP-Link nepodporuje externí připojení antény. Oproti Mercusys má TP-Link vyšší pořizovací cenu.



Obrázek 2 Router TP-LINK TL-WR841N [44]

## Příloha 5c – Popis routeru Netis WF2411

Dalším routerem je Netis WF2411. Tento router disponuje nízkou pořizovací cenou, přenosovou rychlostí, která je oproti TP-Link a Mercusys, 150 Mb/s a jednou anténou se silou 5 dBi.

Obecné parametry routeru Netis jsou:

Model: WF2411

Typ: WiFi Router

Podporované standardy: 802.11b, 802.11g, 802.11n

Typ a počet antén: jedna pevná anténa

Síla antény: 5 dBi

Přenosová rychlost WLAN: 150 Mb/s

Rozhraní: RJ45, WiFi

Frekvenční rozsah: 2,4 GHz

Výrobce: Netis [40]



Obrázek 3 Router Netis WF2411 [40]

## Příloha 5d – Popis routeru ASUS RT-AC1200G+

Posledním routerem použitým při realizaci laboratorní úlohy je router ASUS RT-AC1200G+. Tento router podporuje standard 802.11ac s frekvenčním pásmem 2,4 a 5 GHz a maximální přenosovou rychlostí 1167 Mb/s.

Obecné parametry uváděné výrobcem:

Model: RT-AC1200G+

Typ: Dual-band Router

Podporované standardy: 802.11a (5GHz), 802.11b (2,4GHz), 802.11g (2,4GHz), 802.11n, 802.11ac

Typ a počet antén: 4 pevné antény

Síla antény: 2 dBi

Přenosová rychlost WLAN: 1167 Mb/s

Rozhraní: ASUSWRT

Frekvenční rozsah: 2,4 a 5 GHz

Výrobce: Asus [41]

Při realizaci úlohy se využije počítač Lenovo Z50 -70, ve kterém jsou nainstalované programy Riverbed a Wireshark. Jako kabeláž se využije kabel UTP cat.5 s konektory RJ45.



Obrázek 4 ASUS RT-AC1200G+ [45]

## Příloha 5e - Souhrn parametrů routerů použitých při měření

Tab.1.6: Parametry routerů

Název routeru	Standard	Přenosová rychlost [Mbit/s]	Frekvenční rozsah [GHz]
Mercusys MW301R	802.11b,g,n	300	2,4
TP-LINK model TL-WR841N	802.11b,g,n	300	2,4
Netis WF2411	802.11b,g,n	150	2,4
ASUS RT-AC1200G+	802.11a (pro 5GHz), 802.11b,g,n,ac	1167	2,4   5

## **Příloha 5f – Obsah přiloženého CD média**

Příloha obsahuje skript wifijammer, který je použit v druhé laboratorní úloze. Dále obsahuje naměřené a do grafů zpracované výsledky z měření pro RPi Zero, RPi 3 a RPi 4. A také obsahuje projekt v programu Riverbed, který byl využit při testování v první laboratorní úloze.